INFORMATION ASSURANCE PLATFORM INFORMATION TECHNOLOGY GUIDEBOOK

Prepared by:

Air Force Platform IT Working Group

February 23, 2011

Version 1.2

This Guidebook will be updated periodically

WARNING
INFORMATION SUBJECT TO CONTROL LAWS

This document contains information subject to the International Traffic in Arms Regulation (ITAR)/the Export Administration Regulation (EAR) of 1979, which may not be exported, released, or disclosed to foreign nationals inside or outside the US without first obtaining an export license. A violation of the ITAR or EAR may be subject to a penalty of up to 10 years imprisonment and a fine of $1,000,000 under 22 U.S.C. 2778 or Section 2410 of the Export Administration Act of 1979. Include this notice with any reproduced portion of this document.

NOTICE TO ACCOMPANY THE DISSEMINATION OF EXPORT CONTROLLED TECHNICAL DATA

Export of the attached information (which includes, in some circumstances, release to foreign nationals within the US) without first obtaining approval or license from the Department of State for items controlled by the ITAR, or the Department of Commerce for items controlled by the EAR, may constitute a violation of law.

Under 22 U.S.C. 2778, the penalty for unlawful export of items or information controlled under the ITAR is up to 2 years imprisonment, or a fine of $100,000, or both. Under 50 U.S.C. appendix 2410, the penalty for unlawful export of items or information controlled under the EAR is a fine of up to $1,000,000, or five times the value of the exports, whichever is greater; or for an individual, imprisonment of up to 10 years, or a fine of up to $250,000, or both.

In accordance with your certification that establishes you as a ”qualified US contractor,” unauthorized dissemination of this information is prohibited and may result in your disqualification as a qualified US contractor, and may be considered in determining your eligibility for future contracts with the DoD.

The US Government assumes no liability for direct patent infringement, or contributory patent infringement, or misuse of technical data.

The US Government does not warrant the adequacy, accuracy, currency, or completeness of the technical data.

The US Government assumes no liability for loss, damage, or injury resulting from manufacture or use for any purpose of any product, article, system, or material involving reliance upon any or all technical data furnished in response to the request for technical data.

If the technical data furnished by the US Government will be used for commercial manufacturing or other profit potential, a license for such use may be necessary. Any payments made in support of the request for data do not include or involve any license rights.

Include a copy of this notice with any partial or complete reproduction of these data that are provided to qualified US contractors.

DESTRUCTION NOTICE: For unclassified, limited documents, destroy by any method that will prevent disclosure of content or reconstruction of the document.

Record of Changes

Version	Effective Date	Summary
1.0	12 Nov 2010	Original Document
1.1	18 Nov 2010	-Added clarification to Question 3 of the PIT Determination Checklist -Minor changes to Appendix B -Latest input from ICS for Appendix D -Changes to Appendix E -Minor changes to Appendix F
1.2	23 Feb 2011	-Changed Distribution Statement from D to C for overall PIT Guidebook -Changed Distribution Statement from E to C for the Medical Appendix -Added Air Force logo to title page -MAC wording addition to para. 5.1 (minor change for clarification) -Added this Record of Changes -Corrected PIT Approval figure

Table of Contents

1.0 Introduction

1.1 Purpose

This Platform Information Technology (PIT) Guidebook provides clarity on the Information Assurance (IA) activities required for all systems designated as PIT. This includes weapon systems, medical systems, industrial control systems, test systems, etc., that qualify as a PIT. This PIT Guidebook should be used to develop local procedures that correspond with the product being developed or procured. This PIT Guidebook suggests best practices to be followed in ensuring IA is "built-in" to the product, but allows local variations.

1.2 Executive Summary

The PIT Guidebook is intended to provide Program Managers (PMs) and engineers of PIT systems the information required to ultimately achieve PIT Certification and Accreditation (C&A) from their system's PIT Certifying Authority (CA) and PIT Designated Accrediting Authority (DAA). While local procedures and processes are acceptable, the guidebook establishes the framework that all PIT systems will follow. There are two major processes for PIT, the Acquisition process for new development and the process for legacy, Commercial-off-the-Shelf (COTS), Government-off-the-Shelf and modified-off-the-Shelf. The COTS process is detailed in Appendix B. For weapon systems, the Acquisition process applies and is detailed in Appendix C. Systems engineering including the risk management approach are key to ensuring an IA safe and secure system for both COTS and Acquisition systems. This PIT Guidebook is for Collateral systems only. It does not apply to Special Access Programs/Special Access Required systems, Research, Development, Test, and Evaluation systems or Space systems.

1.3 PIT Definition

PIT is considered a special purpose system which employs computing resources (i.e., hardware, firmware, and optionally software) that are physically embedded in, dedicated to, or essential in real time to the mission performance. It only performs (i.e., is dedicated to) the information processing assigned to it by its hosting special purpose system. Examples include but are not limited to: certain medical devices, industrial control systems, training simulators, diagnostic test and maintenance equipment, aircraft, command and control systems, and many others that do not have a direct connection to the Global Information Grid (GIG). If a connection exists to the GIG, that connection is considered a PIT Interconnection (PITI).

1.4 References

1.4.1 DOD References

a. DoD Directive (DoDD) 5000.01, The Defense Acquisition System, May 2003

b. DoD Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System, December 2008

c. DoDD 8500.01E, IA Policy, April 2007

d. DoDI 8500.2, IA Implementation, February 2003

e. DoDI 8510.01, Information Assurance Certification and Accreditation Process (DIACAP), November 2007

f. Risk Management Guide for DoD Acquisition, Sixth Edition, Version 1.0, August 2006

g. SAF/CIO A6 Memo, PIT, June 2010

h. Defense Intelligence Agency (DIA) Instruction 5000.002, Defense Intelligence Agency

i. Defense Acquisition Guidebook, Defense Acquisition University

j. AFI 33-210, Air Force (AF) C&A Program, 23 December 2008

1.4.2 Other References

a. National Institute of Standards (NIST) Special Publication 800-53, Recommended Security Controls for Federal Information Systems (IS) and Organizations

b. IA Risk Assessment Process, Proceedings of the 2002 Institute of Electrical and Electronic Engineers Workshop on IA, United States Military Academy, West Point NY June 2005, Ken Montry and Rick Kelley

c. Information Assurance Risk Assessment Process for Military Systems White Paper, SENTAR (www.sentar.com), August 18, 2008, Deborah Williams and Larry Johnson

d. NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal IS, February 2010

e. NIST Special Publication 800-30, Risk Management Guide for Information Technology (IT) Systems, July 2002

f. NIST Special Publication 800-60, Guide for Mapping Types of Information and IS to Security Categories

1.5 Background

There is conflicting DoD and Air Force guidance regarding compliance with IA. According to policy references (a and b), acquisition managers shall address IA requirements for all weapon systems; Command, Control, Communications, Computers , Intelligence, Surveillance, and Reconnaissance systems; and information technology programs which depend on external information sources or provide information to other DoD systems.

However, reference (c and j) states this policy does not apply to weapons systems or other IT components, both hardware and software, that are physically part of, dedicated to, or essential in real time to a platform's mission performance where there is no Platform IT Interconnection (PITI). This implies IA is not required for systems that have been determined to be PIT. What this really means is that DIACAP is not required for systems that have been designated PIT unless there is an interconnection to the GIG but IA is required for all systems that incorporate IT.

Due in part to the lack of clear guidance on PIT systems, the Secretary of the Air Force (SAF)/XC, now SAF/Chief Information Officer (CIO) A6, chartered a PIT Working Group to develop policy and procedures which would apply to PIT. An IA program is in fact required for PIT. This guide serves as the model for the actions required to ensure IA is woven into the PIT program, help the PM determine what is PIT versus a PITI and what official channels are required to permit fielding of the PIT or PITI. AFI 33-210 (ref j) is in the process of being revised to better define the role of PIT.

2.0 Roles and Responsibilities

2.1 Program Manager

The PM is responsible to ensure all IA aspects of the program are scheduled appropriately to meet the ultimate goals of IA compliance. The PM needs to comply with the Title 40/Clinger-Cohen Act (CCA) (see Enclosure 5, Table 8 of Reference (b)). The CCA applies to all IT investments. There are IA reporting requirements which will vary depending on the program that are a part of the CCA. These include: CCA #8- Information Assurance Strategy (IAS) discussion in the Information Support Plan; CCA #9-an IAS must be written; CCA#11-register the system in the Enterprise Information Technology Data Repository (EITDR) as PIT. The PM is also responsible to ensure the following tasks are accomplished:

- PIT designed to comply with IA requirements
- Establish a PIT integrated product team
- Perform an IA risk assessment of the system
- Ensure all IA testing requirements are performed
- Follow and obtain the PIT C&A

2.2 Multi-Disciplined Integrated Product Team (IPT)

The IPT for IA should be identified early in the program. The IPT should typically consist of the PM, engineers, using command representative, security specialist, testing community, and others as required. The IPT is concerned with the IA requirements, determining IA risk, recommending IA mitigations for the risks, if required, test planning for IA and resolution of any IA problems

with the PIT CA. Industrial Control System and Medical systems will form IPTs in accordance with their local procedures.

2.3 PIT Certifying Authority

Certification – A comprehensive analysis of the technical and non-technical aspects of an information system in its operational environment to determine compliance to stated security requirements and controls.

The PIT CA is the Technical Authority for the IA aspects of a PIT system within their control. The CA is responsible for ensuring IA requirements are well defined at the earliest stage possible. The CA is then responsible to ensure the IA requirements are implemented to the extent possible based on program or system cost, schedule, and technical tradeoffs. One of the primary functions of the CA is to review the Risk Assessment completed by the IPT. The ultimate goal with the Risk Assessment is to reduce all IA risks to low. The CA should agree with the Risk Assessments accomplished and help structure any mitigations for those risks not considered low. The CA has the responsibility to advise the PIT DAA in making a final IA Risk Assessment of the system or program. CAs are assigned by the AF Senior Information Assurance Officer (SIAO) for PIT systems.

Roles and Responsibilities:

- Focal point for IA policy within the assigned organization
- Coordinates IA related tasks with the AF CIO, Air Staff, National Security Agency, industry counterparts, etc
- Reviews and approves the program IA requirements
- Technical Authority for program-related IA issues
- Formulates their respective organization's IA guidance
- Certifies the system IA design and implementation
- Advises the PIT DAA on IA related issues of the system

Technical Aspects of a System to be Reviewed by the CA:

- System IA Requirements
- Threat Assessment
- Accreditation Boundary
- Data Flow Diagrams
- System Architecture Analysis
- Software, Hardware, and Firmware Design Analysis
- Network Connection Compliance Analysis
- Integrity Analysis of Integrated Products

- Life-Cycle Management Analysis
- Security Test and Evaluation
- Penetration testing requirements
- Emissions Security (aka TEMPEST) and Red/Black Verification Analysis
- Communications Security Compliance Validation
- System Management Analysis
- Vulnerability Assessment
- Supply Chain Risk Management (SCRM) Analysis.

2.4 PIT Designated Accrediting Authority

2.4.1 Accreditation – A management decision by a senior agency official to authorize operation of a PIT-designated system based on the results of a certification analysis and other relevant considerations. The PIT DAA can grant System Accreditation but cannot grant connection approval to the AF GIG. Only the AF- DAA may grant an Authority to Connect (ATC). The current AF-DAA is headquartered at Space Command.

The PIT DAA is a senior official (usually a General Officer or equivalent) that has the authority to take information risk for a program that falls under their purview within their organization. The DAA must be independent of any particular program, but has the authority to influence programs from a global perspective. The DAA consults with the CA in making decisions, but is not bound by the recommendation of the CA. The DAA takes into account the technical, programmatic, and Using Command's needs in rendering a decision. The PIT DAA may issue an Interim Authority to Test (IATT), an Interim Authority to Operate (IATO), and Authority to Operate (ATO) or may deny any of these if necessary. The PIT DAA is appointed by SAF CIO/ A6. Currently appointed PIT DAAs are: ASC/CA (Aircraft Systems); ESC CTO (C2 Systems); AFMSA/CC (AF Medical Services AIS). ICS and Air Armament Center (AAC) requests are in progress.

2.4.2 Responsibilities of the DAA

- Ensure IA requirements are identified and integrated into the systems engineering and acquisition processes as appropriate
- For systems that have an IAS, coordinate on the IAS if requesting a PIT Determination decision
- For systems without an IAS, makes a PIT Determination decision
- Ensure compliance with CCA reporting requirements for IA
- Review/approve the Accreditation Decision Package to include an IA Risk Assessment and Mitigation approach
- Accredit/Deny system for test or operation

- System accreditation package submission to the AF DAA for network connection to the GIG (if required) and acknowledge any PITI in their accreditation decisions

2.4.3 PIT DAA Decisions

The PIT DAA may grant the following accreditation decisions:

1. **IATT**: Special case for authorizing testing in an operational information environment or with live data for a specified time period. An IATT is for testing purposes only.
2. **IATO**: A temporary authorization to operate under the conditions or constraints enumerated in the accreditation decision. An IATO is normally granted for up to one year, with the DAA permitted to extend the IATO period based on program information.
3. **ATO**: Accreditation by the DAA for the system to operate without restriction. All IA risks are considered low or mitigations in place and the DAA agrees that any residual risk is acceptable under the circumstances. An ATO is required prior to Initial Operating Capability (IOC). An ATO may be granted for up to three years.
4. **Denial of Authorization to Operate:** A DAA decision that the information system cannot operate because of an inadequate IA design, failure to adequately implement assigned IA requirements, or other lack of adequate security.

3.0 Platform IT Designation

This chapter provides guidance to the PM in determining if a system qualifies as a PIT system. Per DoDD 8500.1, the C&A process (i.e., DIACAP (ref (e)) is applicable to all AF owned or controlled information systems that receive, process, store, display, or transmit DoD information, regardless of Mission Assurance Category (MAC), classification or sensitivity, except--per DoDD 8500.1 Paragraph 2.3--IT that is considered PIT. PIT designated systems have their own C&A through the assigned PIT CA and PIT DAA.

3.1 PIT Determination Package

A PIT determination package is generally accomplished when sufficient information exists to describe the system and answer the questions in the PIT Determination checklist. This enables the PIT CA and PIT DAA to determine if the system will follow the PIT C&A process or DIACAP. The PIT CA reviews the package and makes a recommendation to the PIT DAA. The PIT DAA then concurs or nonconcurs on the PIT determination. For acquisition programs that will have an IAS, the PIT determination package should be an appendix to the IAS. SAF CIO/A6 approves the IAS, and in so doing, approves the PIT Determination. The PIT Determination Checklist for all systems is below. For programs without an IAS, the below checklist provided by the Air Force Network Integration Center (AFNIC), Scott AFB IL, will be used for the PIT Determination by AFNIC.

3.2 Platform IT Determination Checklist

PURPOSE: Assess the characteristics of IT systems to determine if they are PIT. This checklist does not confer PIT designation without an official Determination Statement issued by the PIT CA/DAA or AF CA.

INSTRUCTIONS: Answer questions in order. Depending upon the responses checked for each question; follow the indicated action.

Question	Responses	If one or more checked	If none checked
(1) Does the IT system or IT component do any of the following with respect to **DoD owned or controlled information systems**? Reference: DoDD 8500.01	☐ Receive ☐ Transmit ☐ Process ☐ Store ☐ Display	CONTINUE WITH QUESTION 2	**STOP.** **There is no Information Assurance Requirement.**
(2) Which of the following describe the IT system or IT component?	☐ It is **physically part of or embedded** in the platform ☐ Its special-purpose mission is **dedicated to** the platform's mission ☐ Its special-purpose mission is **essential in real time** to the platform's mission	CONTINUE WITH QUESTION 3	**STOP** **The IT is not Platform IT** and is subject to the DIACAP C&A process.
(3) Does the mission of the IT **provide <u>general IT services</u>**, such as e-mail, common office applications, networking for one or more non-Platform IT systems, business functions, etc.?	☐ Yes (*Note*: Do not check "yes" if the only possible connection from the IT in question is to another Platform IT system. Also, e-mail and chat used exclusively for tactical operator-to-operator communications with procedures in place limiting the use of e-mail and chat may be part of Platform IT	**STOP** **The IT is not Platform IT** and is subject to the DIACAP C&A process.	CONTINUE WITH QUESTION 4

Question	Responses	If one or more checked	If none checked
	systems.) If so, check "**No**".		
(4) Does the IT system or IT component perform any of these **special-purpose missions?**	☐ Weapon System ☐ Training Simulation ☐ Diagnostic Testing and/or Maintenance ☐ Research and Development (R&D) of Weapon Systems ☐ Calibration ☐ Medical Technology ☐ Transportation ☐ Industrial Control Systems/SCADA Systems ☐ Utility Distribution, such as for Water or Electric ☐ Fire control and targeting; missile; gun; active EW; decoy; launcher; vehicle; artillery; man-deployable system; flight, bridge, classroom training simulator; ☐ Sensor (acoustic, passive EW, ISR, national, control, navigational); radar; P2P or LOS data link; voice comm.; IFF; C2 of forces; navigation system; GPS; displays/consoles; tactical support database or decision aid; some mobile PCs	**The IT is considered to be Platform IT** and is exempt from the DIACAP C&A process, but still must incorporate IA. **CONTINUE WITH QUESTION 5** .	**STOP** **The IT does not appear to be Platform IT** and is subject to the DIACAP C&A process. If the PM/IAM is still unclear as to whether the IT is Platform IT, the PM may submit program and technical information to the AF-CA for an official determination.

Question	Responses	If one or more checked	If none checked
(5) Does the IT in question have any interconnection to a non-Platform IT system? (Note: If the configuration of the Platform IT system changes, the new changes must be addressed with this guide)	☐ Yes	The interconnection is subject to the DIACAP C&A process. Submit the package to the AF-CA.	The IT is required to incorporate IA controls but is not subject to the DIACAP C&A process. Follow IA PIT C&A guidance. Submit this package to the PIT CA for concurrence and the PIT DAA for formal determination approval. Email copy of PIT DAA's formal approval and package to AFNIC/EV.

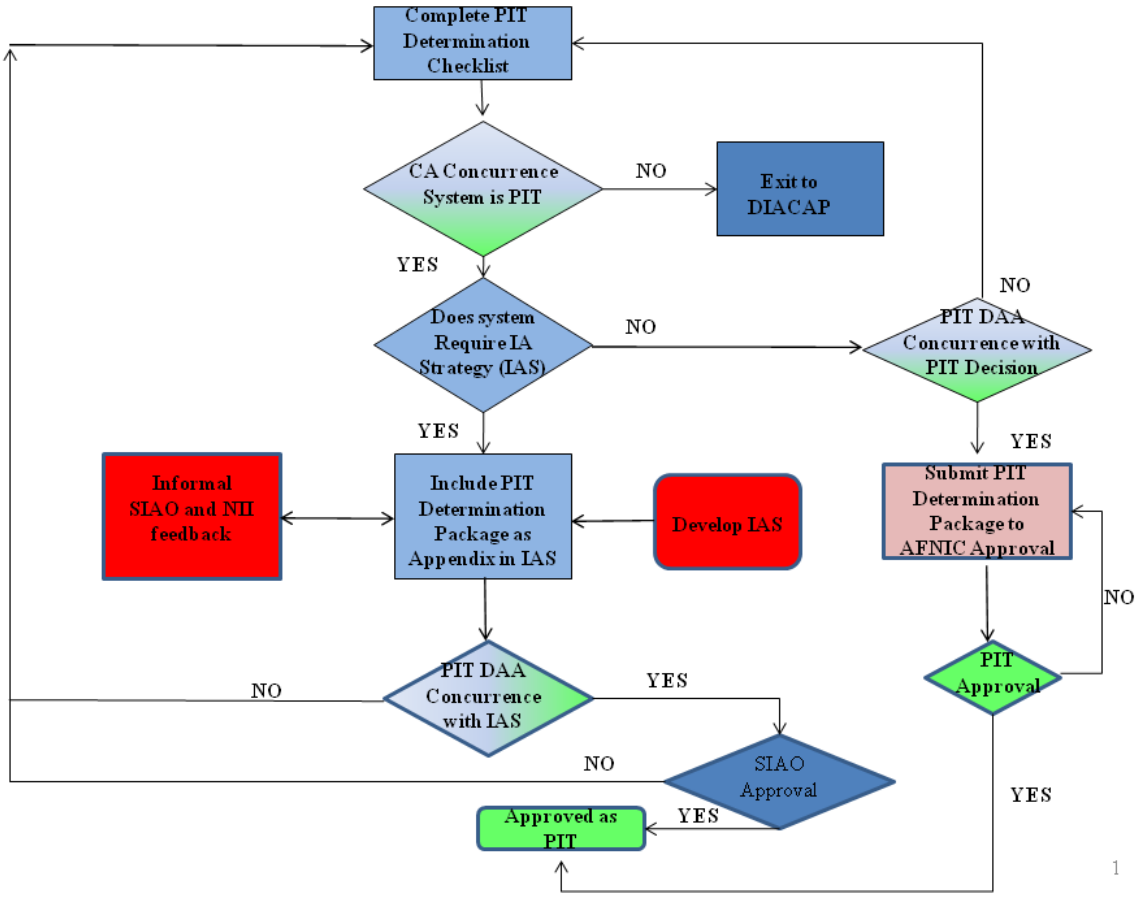
3.2.1 Package Composition

The PIT package consists of a completed PIT Determination checklist (Appendix B and the required artifacts to allow an informed decision by the PIT CA and PIT DAA. Since the PIT determination is accomplished early in the program, many of the artifacts will be notional. The PIT designation can always change as the program matures and more information is known. The artifacts required along with the PIT Determination checklist consists of:

- System Description
- Accreditation boundary
- Data flows and architecture diagrams (DoDAF v2.0 may be utilized for most diagrams)
- Internal and external interfaces
- Controlled interface description
- Identify the CA and DAA

3.2.2 PIT Determination Approval Process

The below flowchart shows the steps required to obtain a PIT determination. It shows both with and without an IAS. An IAS is utilized in most cases for an acquisition program that follows the 5000 series of regulations. With an IAS, once the SIAO has approved the IAS with the PIT determination package, then that constitutes PIT approval. Without an IAS, the PIT determination package is sent to the AF CA (AFNIC/EV) for their concurrence as a PIT.



PIT Determination Flow

4.0 Enterprise Information Technology Data Repository (EITDR) Requirements for PIT

4.1 Requirement

All IS need to be registered in the EITDR. The EITDR feeds the DoD IT Registry. The portfolio manager is normally responsible for the registration. PIT systems are also required to be registered since they are still considered to be an information system. There are hundreds of questions that are usually answered by information technology programs, but for PIT systems there are approximately twenty questions. The PIT system will follow the Warfighter Mission Area and PIT track in answering the questions.

4.2 EITDR Process

The PM or portfolio manager should contact the local CIO office for information on obtaining access to the EITDR database and timeframe required to submit EITDR information.

5.0 PIT IA Requirements

5.1 General IA Requirements

The IA requirements are derived from DoDI 8500.2, NIST SP 800-53 and system specific requirements are generated for the system or item in question. PIT has the flexibility to tailor the appropriate requirements or IA controls and not just use a canned set of controls, such as in the DIACAP method. Many of the controls listed in DoDI 8500.2 are not applicable for PIT systems, may be tailored to the particular system or system specific requirements may be developed to ensure the security of the system. MAC is directly associated with the importance of the information and is determined by the warfighters' requirements. While MAC is not that important for Platform IT systems, MAC I, II or III controls form a good baseline in establishing integrity and availability controls. A Systems Requirement Traceability Matrix (SRTM) is normally generated to baseline the IA requirements (controls), no matter how generated for the system in question. Non-acquisition programs may have their own set of controls that are deemed necessary for their system. The tailored requirements are approved by the CA and DAA.

5.2 PIT Alternative Requirements Method

The NIST Risk Management Framework (NIST SP 800-37) allows two methods of selection IA controls, baselines, and profiles. Each has its advantages and disadvantages. Both allow for a certain degrees of consistency across similar systems, especially within a community; but, the more specialized your system is, the more reciprocity is jeopardized. Baselines are established by first categorizing the information type, such as is done with NIST SP 800-60. Unfortunately, DoD does not have an equivalent publication which categorizes information. The primary advantage of baselines is that there are no Not Applicable (N/A) controls to justify, as you select only the controls you need for the information type. Conversely, profiles establish the set of controls for a given system type, but you may not need all the controls to address the specific threats and vulnerabilities for your system. Therefore, you will likely need to justify why some or many of the controls are N/A. The more specialized your system is, the more likely you'll have more N/A controls. In that case, it makes more sense to use the baseline approach. Either approach is valid, and you must evaluate which is better, achieving reciprocity by using a profile, or not justifying N/As by using the baseline. These alternative methods maybe of use as the DoD transitions to utilizing the NIST standards in the future.

6.0 PIT Risk Management is the process of identifying risk, assessing risk, and taking steps to reduce risk to a level acceptable to a PIT DAA. Risk is a function of the likelihood of a given threat exercising a potential vulnerability and the resulting impact. There are three components of PIT IA Risk:

- A future root cause (manifested by a specific threat and vulnerability), which, if eliminated or corrected, would prevent a potential consequence from occurring
- A probability (or likelihood) assessed at the present time of that future root cause occurring
- The consequence (or effect) of that future occurrence

Threat is the intent and/or capability of an adversary to adversely affect (cause harm or damage to) the PIT system. Vulnerability is a flaw or weakness of the PIT system that can be intentionally or unintentionally exploited by one or more specific threats. A threat does not present a risk to a PIT system when there is no vulnerability that can be exploited.

6.1 PIT IA Risk Management. PIT IA Risk Management is modeled after the Risk Management process model from the Risk Management Guide for DoD Acquisition and includes the following steps:

Step 1. Risk Identification

Step 2. Risk Analysis

Step 3. Risk Management Planning

Step 4. Risk Mitigation Plan Implementation

Step 5. Risk Tracking

CAUTION. Before executing the steps in the PIT IA Risk Management Process below, it is wise to consider the security classification level of the results and select an appropriate venue to host, process and store PIT IA Risk Management data.

6.2 Risk Assessment IPT. The purpose of this IPT is to bring system stakeholders together to provide a forum for continually identifying and assessing PIT IA risk throughout system design and operation. This IPT will recommend solutions to the PM. The IPT should include all the necessary stakeholders, internal and external. Each program can choose its own IPT members, but the IPT should include program engineering, system security engineering, using MAJCOM, test organizations, and a CA representative. It is recommended that the Chief/Lead Engineer serve as the chairperson for this IPT.

The remainder of this section will describe the key steps and the specific actions that the Risk Assessment (aka "Risk") IPT should undertake.

6.3 Step 1. Risk Identification. Risk Identification is accomplished in a series of actions that determine root cause by identifying threats and system vulnerabilities, pairing threats and system vulnerabilities, and creating specific risk statements for each root cause pairing.

6.3.1 Action 1. Threat Identification. In order to determine root cause for PIT, the threats to the PIT system and its operational environment must be understood. The result of this action should be clear and concise threat statements that capture circumstances or events with the

potential to intentionally or unintentionally cause an incident affecting the availability, integrity, authentication, confidentiality, and non-repudiation of a system. It may be helpful to create a Risk Assessment table at this point to capture results. Threats are identified in the rows of the table, vulnerabilities in the columns, and each intersection potential risks.

Threat Sources. Threats can be categorized as internal or external. Internal threats are the result of individuals with malicious intent or plain mistakes in operating the system. External threats are the result of outside sources trying to disrupt US DoD operations. The external threat is generally an orchestrated attempt by a foreign government.

Capstone Threat Assessment (CTA). CTAs address, by warfare area, current and future foreign developments that challenge US warfighting capabilities.

System Threat Assessment Report (STAR)/System Threat Assessment. Appropriate Defense Intelligence organization(s), identified by DIA, prepare the STAR. The assessment should be system specific to the degree that the system definition is available at the time the assessment is being prepared. The assessment should address projected adversary capabilities at system IOC and at IOC plus 10 years.

6.3.2 Action 2. Vulnerability Identification and Analysis. The goal of this action is to identify all threat vectors or paths a threat may take to exploit the system. This will be described as a characteristic of the system that makes it vulnerable to an IA threat. DIACAP is focused on identify security "weaknesses". The term security weakness is not well defined, but is commonly understood to refer to IS non-compliance to a specific IA control. These security weaknesses may be used as a basis to identify system vulnerabilities. **Section 5.0** of the PIT Guide addresses the development of a SRTM. The SRTM identifies all IA requirements (e.g. DIACAP, NIST, system unique) applicable to the system.

The PIT system should be assessed against each requirement or control to determine its level of compliance. If non-compliant, this security weakness should be further evaluated to determine if it represents system vulnerability. If a threat statement cannot be linked to at least one vulnerability, a root cause does not exist the threat should be removed from further consideration. Similarly, if a threat-vulnerability relationship cannot be established for each non-compliant requirement, then the non-compliant requirement does not pose a risk to the system and should be removed from further evaluation. This does not represent a failure in the process only that at the time the IA requirement was established, system specific information led to the application of a requirement that may have driven the system to a higher security posture than necessary to counter the threat.

In addition, as the program matures through systems engineering, vulnerabilities may be discovered that are outside the scope of identified requirements. These vulnerabilities must not be dismissed and should be used to develop risk statements if a linkage to a specific threat can be

made. Vulnerabilities should be entered as columns in the Risk Assessment table from Action 1, and a simple "X" placed in the corresponding threat intersection(s) (later in Action 3, these will be replaced with a risk id number (R1, R2, R3, etc.)). Multiple risks may be associated with a single threat and vulnerability intersection.

The results of this action are clear and concise vulnerability statements describing a flaw or weakness in design or implementation, including security procedures and controls, and the linkage of each vulnerability to at least one threat.

6.3.3 Action 3. Write Risk Statements. Capturing a statement of risk involves considering and recording the conditions that are causing concern for a potential loss to the system. Risk statements must be neutral, clear, quantifiable statements. The objective of capturing a statement of risk is to arrive at a concise description of risk, which can be understood and acted upon. The components and description of a statement of risk are:

- condition: a single phrase or sentence that briefly describes the key circumstances, situations, etc., causing concern, doubt, anxiety, or uncertainty
- consequence: a single phrase or sentence that describes the key, possible negative outcome(s) of the current conditions

Again, risk statements must be linked to specific threats and vulnerabilities. The combination of a specific threat and vulnerability may result in one or many risk statements. Risk statements should be maintained in the risk assessment table (for example as a separate tab if using Microsoft Excel) and given a unique identifying number (e.g. R1, R2, R3). The unique identifying number should replace the placeholder "X" (Action 2) in the corresponding threat-vulnerability intersection.

The result of this action will be a number of unique risk statements, each specifically mapped to a threat and vulnerability. Risk statements should also be associated with its' associated IA control/requirement in the SRTM.

Step 1 Summary. As a result of the actions in Step 1, *Risk Identification*, the Risk IPT should have generated a list of system specific threats, identified system vulnerabilities linked to specific threats, and developed corresponding risk statements that capture the essence of the question "What could go wrong?" The results of Step 1 should have been captured in a risk assessment table. At this point is it advisable to vet the information outside the Risk IPT, to include the PM and PIT CA. The PIT CA will determine if the information warrants presentation/exposure to the PIT DAA.

6.4 Step 2. Risk Analysis. Risk analysis involves determining and assigning an appropriate probability or likelihood of occurrence and consequence of occurrence to each of the identified risks from risk identification activity. The goal is to answer the question "How big is each risk?"

6.4.1 Action 1. Assign Probability Risk Factor.

The likelihood of occurrence is one of the more difficult attributes to assign. Determining an actual probability of occurrence of an attack on a PIT system would most likely be dynamic over relatively short periods of time (as compared to a procurement cycle). Instead, assigning a probability of occurrence based on a relative scale, taking into account an estimation of the means and opportunity of a potential adversary is more feasible.

Means. Means represents an estimation of an adversary's difficulty in creating the conditions necessary for a risk occurrence. An attack is an action intended to compromise the confidentiality, integrity, and or availability of a PIT system. There are many types of attacks including intrusions, reconnaissance, tampering, implantation, denial of service, corruption of data, ex-filtration of data, etc.

Opportunity. Opportunity represents an estimation of an adversary's accessibility to exploit a PIT system. A system's attack surface is the set of methods or interfaces through which an adversary can enter the system and conduct an attack. Opportunity is an estimation of a system's attack surface.

Each risk is assessed for both means and opportunity and assigned means and opportunity levels according to the criteria in Tables 1 and 2 found in Appendix G. Each table contains two columns. Either column may be used depending on the subject area of the IA control that the risk is based upon. As always, the best judgment of the Risk IPT should prevail.

This is a tedious process as each risk must be assessed against the criteria. It is recommended that the Risk IPT Lead allow sufficient time to accomplish and vet each risk by the IPT members. The risk assessment table "risk tab" generated in Step 1, *Risk Identification*, should be used to track mean and opportunity levels against each risk.

With the aid of the Probability Risk Factor Matrix (Figure 1), individual means and opportunity levels are used to determine an overall Probability Risk Factor Level for each risk. This overall Probability Risk Factor Level should be tracked in the "risk tab".

Probability Risk Factor Matrix						
Opportunity						
Means		O-1	O-2	O-3	O-4	O-5
	M-5	**2**	**3**	**5**	**5**	**5**
	M-4	**2**	**3**	**4**	**5**	**5**
	M-3	**1**	**2**	**3**	**4**	**5**
	M-2	**1**	**2**	**3**	**4**	**4**
	M-1	**1**	**1**	**2**	**3**	**4**

Probability Determination		
Level	Likelihood	Probability of Occurrence
1	Not Likely	~10%
2	Low Likelihood	~30%
3	Likely	~50%
4	Highly Likely	~70%
5	Near Certainty	~90%

Figure 1 Probability Risk Factor Matrix

The result of this action is an updated Risk Assessment table that includes the mean and opportunity assessments for each risk statement. Using the mean and opportunity levels an overall Probability Risk Factor level was determined for each risk.

6.4.2 Action 2. Assign Consequence Risk Factor.

A consequence is the outcome of a risk occurrence. The consequence of occurrence is unique to each system. The consequence needs to take into consideration not only the impact on the system in question, but how critical the occurrence impacts not just the PIT system itself but also on dependent systems. In general, consequences are not affected by system design changes. The consequence could still be realized, the mitigation just lowered the probability of this risk occurring. For this approach, consideration needs to be given to both the impact and criticality of the risk manifestation, and based on these levels, determine the overall consequence to the system.

Impact. Impact represents an estimation of the effect or consequence that may result from an attack on the system resulting in a specific risk occurrence.

Criticality. Criticality represents an estimation of the change in the PIT system performance and the relationship of this change on dependent systems.

Each risk is assessed for both impact and criticality and assigned levels according to the criteria in Tables 3 and 4 found in Appendix G. Each table contains two columns. Either column may be used depending on the subject area of the IA control that the risk is based upon. As always, the best judgment of the Risk IPT should prevail. The Risk Assessment table "risk tab" generated in Step 1, *Risk identification*, should be used to track impact and criticality levels against each risk.

With the aid of the Consequence Risk Factor Matrix (Figure 2), individual impact and criticality levels are used to determine an overall Probability Risk Factor Level for each risk. This overall Consequence Risk Factor Level should be tracked in the "risk tab".

Consequence Risk Factor Matrix						
Criticality						
Impact		C-1	C-2	C-3	C-4	C-5
	I-5	**2**	**3**	**4**	**5**	**5**
	I-4	**2**	**3**	**4**	**4**	**5**
	I-3	**1**	**2**	**3**	**4**	**5**
	I-2	**1**	**1**	**2**	**3**	**4**
	I-1	**1**	**1**	**1**	**2**	**3**

Consequence Determination	
Level	Consequence
1	Negligible
2	Minor
3	Moderate
4	Major
5	Catastrophic

Figure 2 Consequence Risk Factor Matrix

The result of this action is an updated Risk Assessment Table that includes the results of the Risk IPT assignment of impact and criticality criteria for each risk statement. These criteria were applied to a Consequence Risk Factor Matrix and an overall Consequence Risk Factor was generated for each risk.

6.4.3 Action 3. Assign Overall Risk Factor.

This action will use the Probability Risk Factor and Consequence Risk Factor Levels to determine an Overall Risk Factor for each risk using the Overall Risk Factor Matrix (Figure 3). The Overall Risk Factor value (Low, Moderate, or High) should be tracked in the "risk tab".

Overall Risk Factor Matrix						
Consequence						
Probability		1	2	3	4	5
	5	**Low**	**Moderate**	**High**	**High**	**High**
	4	**Low**	**Moderate**	**Moderate**	**High**	**High**
	3	**Low**	**Low**	**Moderate**	**Moderate**	**High**
	2	**Low**	**Low**	**Low**	**Moderate**	**Moderate**
	1	**Low**	**Low**	**Low**	**Low**	**Moderate**

Figure 3 Overall Risk Factor Matrix

The result of this action is an updated Risk Assessment table that indicates an Overall Risk Factor level for each risk statement.

6.4.4 Action 4. Risk Analysis Results Reporting.

It is advisable to report results to the CA and DAA and obtain PIT CA and DAA guidance on their specific risk mitigation policy. The Risk IPT should not assume that all risks must be mitigated to low or the system cannot proceed to the next phase if a high risk exists. The PIT CA and DAA may issue broad guidance such that all high risks must be mitigated to low, or issue guidance on specific risks, or something in between.

In some cases, it may be desirable to prioritize risks within each Overall Risk Factor value. This may help to focus activities for Step 3, *Risk Management Planning*. It may also be desirable to create alternative views (either graphic or tabular) depicting relationships between IA requirements, threats, vulnerabilities, and risks. Low risks are generally regarded as risks to be accepted, but this understanding should be confirmed with the PIT CA and DAA, as other factors may be of concern. Low risks may have achieved this level due to an aspect or design detail of the system seemingly unrelated to security. It is important to document this "mitigation" under Step 3, in the event this feature is modified or deleted from the system. Figure 4 depicts the rollup of the Consequence Risk Factor and Probability Risk Factor into the Overall Risk Factor Matrix.

How these results are reported will vary depending upon CA and DAA preferences, but it is desirable to present information to the CA and DAA in a common and consistent manner across all PIT systems. Figure 5 is an example of a standard risk reporting template that has been used successfully within Aeronautical Systems Center. The residual risk factor and the information conveyed to the DAA in the accompanying text must be a clear risk statement (including consequence) that the Risk IPT and PIT CA are recommending that the PIT DAA accept.

The results of this action will help to ensure all stakeholders (PM, Chief Engineer, CA, DAA, System User, etc.) agree with the results of the Risk IPT and have an understanding and appreciation of how requirements, threat, and vulnerabilities contribute to the Risk level of the PIT System. There should also be clear understanding of the PIT DAA risk acceptance policy.

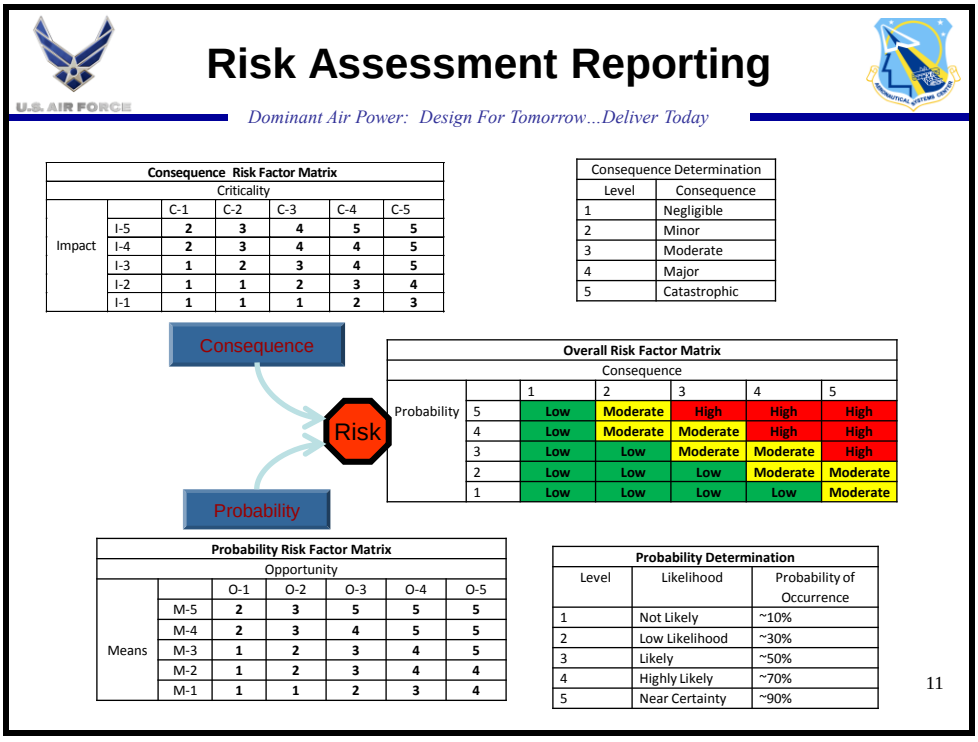


Figure 4 Risk Factor Rollup

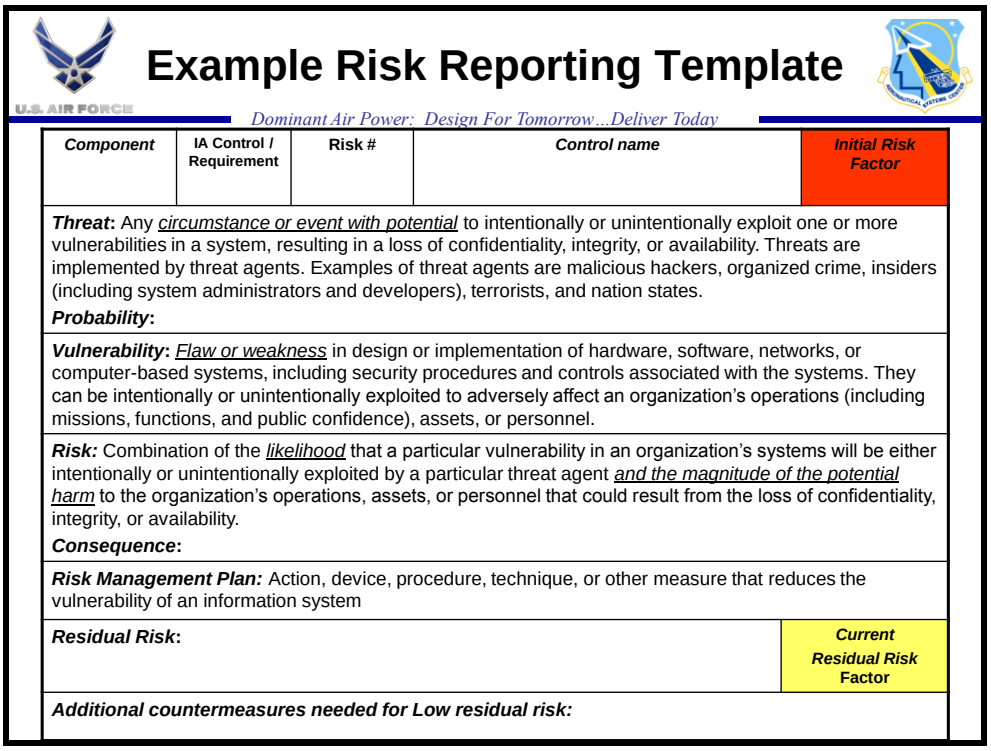


Figure 5 Example Risk Reporting Template

Step 2 Summary. As a result of the actions in Step 2, *Risk Analysis*, the Risk IPT has completed a comprehensive risk analysis taking into account the means and opportunity of an adversary to attack the PIT system as well as the impact and criticality of such an attack. An overall Risk Factor has been generated for each individual risk that mirrors the standard Risk Reporting Matrix from the Risk Management Guide for DoD Acquisition. Results have been tabulated and analyzed by the Risk IPT and reported to and agreed upon by the stakeholders.

6.5 Step 3. Risk Management Planning. The goal of Risk Management Planning is to develop an overall PIT system Risk Management Plan which includes specific management plans for each risk. This is accomplished by identifying, evaluating, and selecting management options to set risk at an acceptable level to the PIT CA and PIT DAA. It includes the specifics of what should be done, when it should be accomplished, who is responsible, and required resources to implement. For each risk, one or more of the following management options may apply:

1. Avoiding risk by eliminating threat and/or the consequence. This includes not performing an activity that could carry risk. This could be accomplished by modifying program requirements. This adjustment could be accommodated by change in funding, schedule, or technical requirements. Avoidance may seem the answer to all risks, but

avoiding risks also means losing out on an increased capability that accepting the risk may have allowed. Risk avoidance is difficult to achieve in PIT and therefore not a common mitigation strategy.

2. Controlling and/or reducing system vulnerability. This adjustment could be accommodated by any number of methods including changing the systems design, implementing additional procedures, or increasing user training. This is the most common form of risk management applicable to PIT system. It is synonymous with the term risk mitigation (mitigation - the action of lessening in severity or intensity).
3. Transferring the Risk. Reassign organizational accountability, responsibility, and authority to the PIT system Information System Owner. The conditions of this transfer must be documented in the System Security Plan.
4. Accepting the level of risk. Risk acceptance is solely the responsibility of a PIT DAA under whose mission the PIT system is supporting. IA risk acceptance must be clearly documented by the PIT DAA before a system may commence testing or operations.

It is recommended that the Risk Management Plan be captured in the risk assessment table. A "management" tab should be added to capture this information with the uniquely numbered risks identified in the first column and subsequent columns (e.g. management option, description/details, schedule, Point of Contact, required resources, priority, status date, cost, etc.).

Cost. It is important to capture all associated costs for the risk management option selected. This could not only include the actual near-term dollar costs of implementing but also the life-cycle costs (in terms of operations, maintenance, and training). In addition opportunity cost (in terms of mission impacts (e.g., unavailability of specific functions or capabilities, time lag in performing mission functions, lack of connectivity) and technology constraints (e.g., inability to use a new technology, cost to integrate a new product into legacy architecture) should be captured.

6.5.1 Action 1. For each risk, the Risk IPT must identify the risk management option that will be followed. As mentioned previously, it is important to capture aspects or design details, seemingly unrelated to security, that contribute to the reduction of risk. In the event this feature is modified or deleted from the system, its' impact on the system security can be addressed. The results of this action should be the beginnings of a Risk Management Plan.

6.5.2 Action 2. Completely address all Risk Management Plan topics for each risk.

6.5.3 Action 3. Prioritize risk management options by category based upon cost, schedule and performance, and security impact.

6.5.4 Action 4. Provide Risk IPT recommendations to PM and PIT CA.

6.6 Step 4. Risk Management Plan Implementation. The goal of this step is to ensure the Risk Management Plan is implemented. In general recommendations outlined in the Risk Management Plan must be acted upon. These may impact the system design and configuration or may impact operational procedures and parameters. Step 2, *Risk Analysis*, and Step 3, *Risk Management Planning*, will be required to verify results.

6.7 Step 5. Risk Monitoring and Tracking. The intent of risk tracking is to ensure continued risk management throughout the PIT systems operational life. Periodically reassess by accomplishing Step 1, *Risk Identification* and Step 2, *Risk Analysis*. Accomplish Step 3, *Risk Management Planning*, and *Risk Management Plan Implementation*, if required.

7.0 Supply Chain Risk Management

SCRM is not unique to PIT systems. All DoD systems need to ensure products being procured meet the specification requirements and come from reliable sources. This is not a guide for SCRM, but acknowledges the need to consider SCRM in the development and procurement of PIT systems. Following are topics of interest for SCRM:

- A Risk Assessment is performed to identify the critical components in the information flow of the system
- Key critical parts identified receive special SCRM attention to ensure the source is reliable and not counterfeit
- Prime contractor has a SCRM program in place
- Contractor ensures SCRM requirements are levied to all sub-contractors
- Key critical parts are free of malware or malicious code
- Software used in the system has a known pedigree
- Software used in the system is free of malicious code

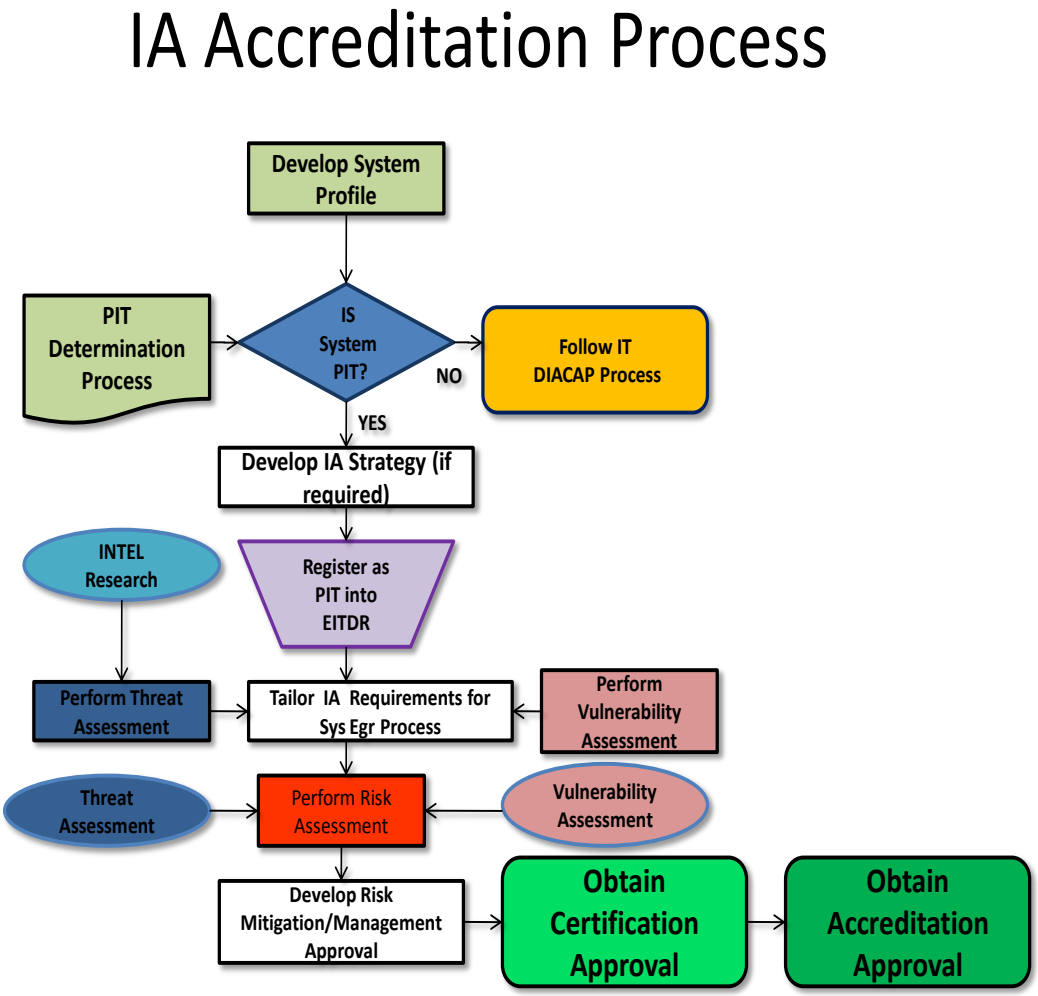
8.0 PIT Interconnection (See Appendix F)

PITI is the interface of each boundary where PIT connects to non-PIT. An accredited system used as PITI must clearly explain the following three features:

- At least one external interface used to connect to PIT systems, networks, or components
- The system's IA protection features serving to separate and protect PIT from non-PIT (usually associated with the external interface(s) used as PITI)
- The PITI is subject to IA policy and certified and accredited by the AF DAA using the DIACAP process.

9.0 IA Accreditation Process

The below flowchart shows the generalized IA Accreditation process that is applicable to all PIT systems. Adapt it for your local procedures and the type of system you are acquiring.



10.0 Reciprocity

Reciprocity as defined by the *DoD memorandum regarding DoD Information Systems Certification and Accreditation Reciprocity* is a "mutual agreement among participating enterprises to accept each other's security assessments in order to re-use IS resources and/or accept each other's assessed security posture in order to share information." It is also noted from the memorandum that "Reciprocity requires a level of trust based on transparency, uniform processes, and a common understanding of expected outcomes."

This guide should provide a uniform process and help develop a common understanding of the outcomes, but transparency will remain a key element in implementation of the principles of reciprocity. Reciprocity is not a blind acceptance of another's accreditation decision; it is the re-use and re-evaluation of existing documentation. Documentation should be made available to aid the accepting CA/DAA evaluation teams. Re-testing and development of new documents should be avoided if the information exists in some form. Since diverse organizations require unique documents to meet their standards it is important to understand that the content of the documentation is the key, not the label on the document.

The DAA is not re-accrediting a system but is making an ATC decision. This decision is based on the amount of risk the new system brings as a result of its current security posture. There may be systems that require the addition of new security requirements such as when the proposed connection changes the existing security structure. An example might be when deciding to connect a system that had previously been autonomous when no requirements had been implemented to mitigate the vulnerabilities presented by a network connection. The modification and testing of any security controls to ensure the system meet the new requirements should be the responsibility of the system owners. Test results and analysis should be made available to aid in final analysis. The final decision regarding acceptance of a previous accreditation resulting in an ATC resides with the accepting DAA.

11.0 Expiration

To ensure the user has the most current up to date guidance available ensure your copy is less than 12 months old based on the cover sheet date. The PIT working group will maintain a current version on the AF PIT Working Group Community of Practice located at: https://afkm.wpafb.af.mil/ASPs/DocMan/DOCMain.asp?Tab=0&FolderID=24787&Filter=24787

IA PIT Guidebook

Appendix A: Acronym List

Acronym	Definition
AF	Air Force
AFNIC	Air Force Network Integration Center (Scott AFB IL)
AFOTEC	Air Force Operational Test and Evaluation Center
AFSIT	Air Force System Interoperability Test
ASC	Aeronautical Systems Center
ATC	Authority to Connect
ATO	Authority to Operate
C4	Command, Control, Communications, and Computers
C&A	Certification and Accreditation
CA	Certifying Authority
CCA	Clinger-Cohen Act
CCB	Configuration Control Board
CDD	Capabilities Development Document
CDR	Critical Design Review
CIO	Chief Information Officer
CL	Confidentiality Level
COMSEC	Communications Security
DAA	Designated Accrediting Authority
DIA	Defense Intelligence Agency

DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
EITDR	Enterprise Information Technology Data Repository
EMD	Engineering and Manufacturing Development
GIG	Global Information Grid
IA	Information Assurance
IAM	Information Assurance Manager
IAS	Information Assurance Strategy
IATO	Interim Authority to Operate
IATT	Interim Authority to Test
ICS	Industrial Control Systems
IMP	Integrated Master Plan
IPT	Integrated Product Team
ISP	Information Support Plan
ISR	Intelligence, surveillance, and Reconnaissance
IT	Information Technology
JITC	Joint Interoperability Test Center
KPP	Key Performance Parameters
MAC	Mission Assurance Category

MAJCOM	Major Command
MS	Milestone
MSA	Material Solution Analysis
NASIC	National Air and Space Intelligence Center
NIST	National Institute of Standards and Technology
PDR	Preliminary Design Review
PIT	Platform Information Technology *also* Platform IT
PITI	Platform Information Technology Interconnection
PM	Program Manager
PPP	Program Protection Plan
PRR	Production Readiness Review
PTPI	Platform IT to Platform IT Interconnection
RFP	Request for Proposal
SAF	Secretary of the Air Force
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
SE	Systems Engineering
SEP	Systems Engineering Plan
SFR	System Functional Review
SIPRNET	Secure Internet Protocol Router Network
SRCM	Supply Chain Risk Management
SRD	System Requirements Document

SRR	System Requirements Review
SRTM	System Requirements Traceability Matrix
SSP	System Security Plan
STAR	System Threat Assessment Report
SVR	System Verification Review
T&E	Test and Evaluation
TD	Technology Development Phase
TEMP	Test and Engineering Master Plan
TEMPEST	Term commonly used to refer to Emissions Security
TPM	Technical Performance Measurement
TRR	Test Readiness Review
US	United States

Appendix B

Platform Information Technology (PIT) Process for Legacy, Commercial-off-the-Shelf (COTS), Government-off-the-Shelf (GOTS) and Modified-off-the-Shelf (MOTS) Systems

1.0 Definitions

1.1 COTS: Equipment procured from one or more vendors that are available to the public or entities of interest. This equipment normally is designed and built to industry standards and not necessarily built to Government specifications. The equipment is used as delivered by the contractor of the equipment.

1.2 GOTS: Equipment previously designed for a Government application and being utilized by another entity. This equipment normally has been procured with a Government specification.

1.3 MOTS: Equipment that could previously be considered COTS or GOTS but is being modified to meet a particular need. Generally it is COTS equipment that is being altered to satisfy a special design application.

1.4 Legacy Equipment: Legacy equipment is existing equipment currently in use and maybe any combination of the above.

2.0 Certification and Accreditation (C&A)

See the below C&A process flowchart for acquisition of COTS, GOTS or MOTS equipment.

2.1 Threat/Vulnerability Assessment: A Threat Assessment should be accomplished even though you may not be able to make any design changes due to the existing equipment. Sometimes procedures may be put in place to mitigate the issues.

2.2 Design Analysis: Vendor information is used to analyze the COTS equipment. A minimum set of Information Assurance (IA) requirements are established that the COTS equipment should meet either by design or procedure.

2.3 Risk Assessment: The risk assessment process as detailed in section 6 of the core PIT Guidebook may be tailored as required to meet the needs of the COTS equipment. Testing should be accomplished to verify the vulnerabilities of the system. Certification Authority and Designated Accrediting Authority concurrence is required for COTS equipment as it is for any PIT system.

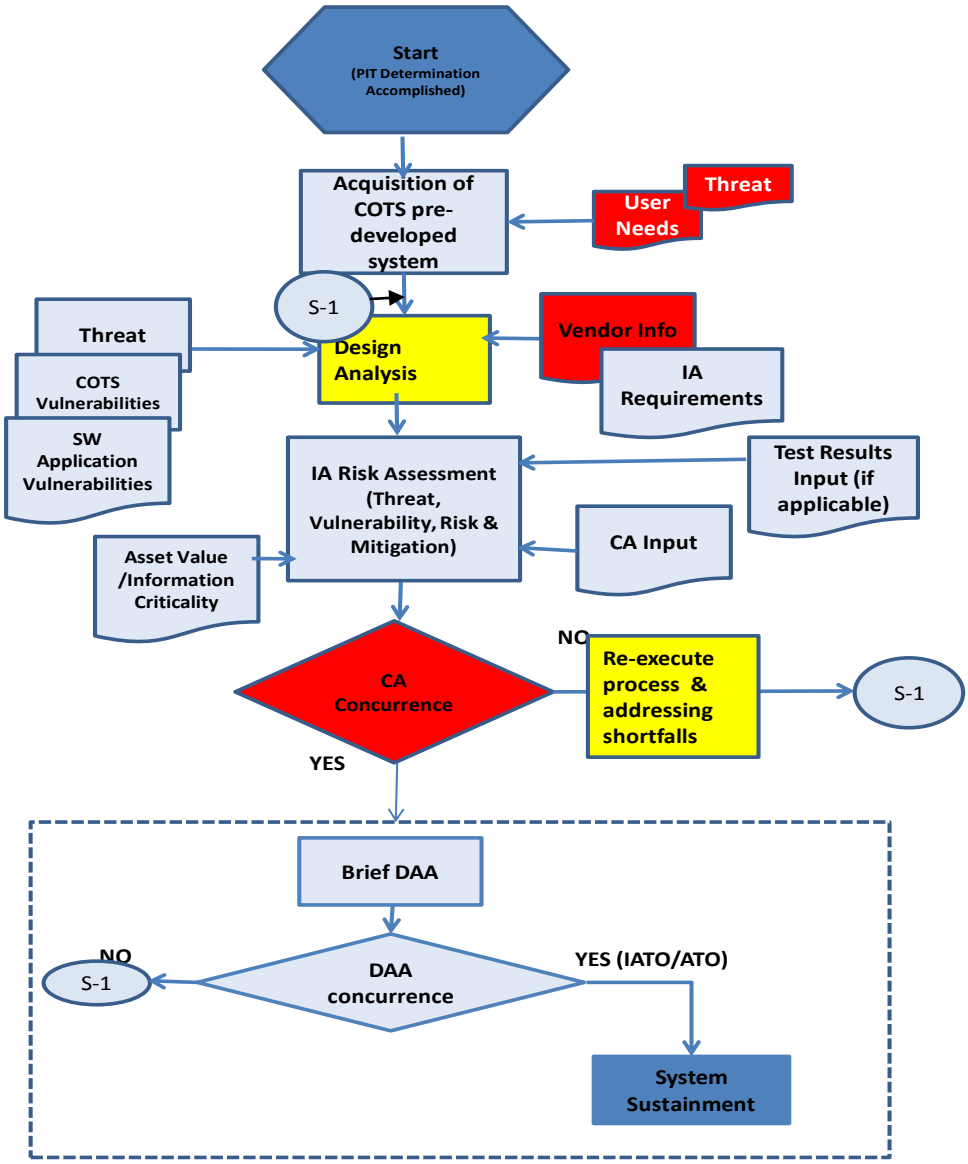
2.3.1 COTS: COTS equipment is normally accepted as is if it meets the performance requirements of the intended use. The risk of using it must be considered in conjunction with the overall program risks. If the inherent risks are unacceptable, external safeguards should be considered before

the COTS solution is not used. The same IA requirements or controls should be analyzed for applicability to COTS.

2.3.2 GOTS: GOTS equipment should be treated the same as GOTS, but it may already have been certified and accredited in another program. The IA requirements that it satisfies should be reviewed to ensure it meets the needs of your particular application.

2.3.3 MOTS: When existing COTS or GOTS is modified, that is good time to ensure IA requirement are met.

2.3.4 Legacy Equipment: The risk of Legacy equipment by its very nature has been accepted sometime in the past. If it meets any IA requirements or controls, these are considered to be inherited. In this case a risk assessment is performed to ensure acceptable risk for the new application.



C&A Process for Legacy, COTS, GOTS, MOTS

Appendix C

Platform Information Technology (PIT) Acquisition Process

This Appendix gives a view of the PIT acquisition process from the system engineering perspective. New acquisition programs that follow the 5000 series of regulations should use this as a guide in developing the IA portion of the program. The following pages outline the steps to be taken and then selected information is detailed to help the user acquire the PIT system and ultimately receive certification and accreditation. Programs may enter the appropriate acquisition phase and perform the necessary steps.

Task Name
Material Solutions Analysis (MSA) Phase
Initial Threat Assessment
STAR
Space Capstone
Air Capstone
Integrated Threat Assessment (From OSI)
Research Other Threats
Continuous Threats Update from Intel
IAS/PIT Determination Package
Program Specific Documents Review
Program Specific Overview Briefing
IA Overview Brief to Program Office
Develop IAS/PIT Determination Package
Determine IA Boundary
Create IAS/PIT Documentation
Peer Review IAS/PIT Determination Package
Program Office Review and Coordination Staff Summary Sheet
CA Review and Coordination
DAA Coordination
SAF/CIO/A6 Approval
Milestone A
Exit Criteria
Initial Threat Assessment
Initial IAS/PIT Package
Technology Development (TD) Phase
Develop IA Requirements for SRD/RFP
Approval of IA Requirements by CA
Develop Data Flow Diagrams
Develop IA stakeholders List (SIP) for IPT
Develop MOA Between DAAs (As Needed)
Updated Threat Assessment
STAR
Space Capstone
Air Capstone
Integrated Threat Assessment (From OSI)
Research Other Threats
Continuous Threats Updates from Intel
Source Selection Plan input/participation (Ensure IA requirements are put in SOW, SOO (Section L and M), S
Review and provide IA inputs to the Program Documents
Perform IA Risk Assessment
EITDR registration
Complete EITDR Questionnaire

Complete Registration and get reference number
SSR
Determine/Review IA Requirements (SRTM)
Determine Data Classification levels for each IA Control
Determine MAC Classification for each IA Control
Determine Weapons System Specific IA Requirements (Controls)
Determine the Validation Procedures for the IA Requirements
Approval of IA Requirements by CA
Risk Analysis
Perform Risk Assessment
Identify threats to the system (from Threat Assessment)
Identify System Vulnerability
Quantify the Probability the Threat can exploit the Vulnerability
Quantify the consequence to the mission should the threat exploit the vulnerability
Quantify the Risk based on probability and consequence
Generate Risk Analysis for each Risk
Develop Risk Mitigation Approach (for each Medium and High Risk)
Develop Risk Mitigation Options
Perform Cost-Benefit Analysis on each proposed mitigation
Generate Summary Risk Matrix
Generate Summary Risk Report
Supply Chain Risk Assessment
HW Components Risk Assessment
Generate HW Components List
Check the HW components for existing vulnerability against vulnerabilities database
Assess Supply Chain Risk for Critical HW components
Identify Risk Mitigation
SW Components
Generate SW components list
Check the SW components for the existing vulnerability against vulnerabilities database
Assess Supply Chain Risk for Critical SW components
Identify Risk Mitigation
Coordination of Risk Matrix/Analysis with CA
SFR
Update Data Flow
Update Risk Analysis
Update Risk Assessment
(Update) Identify threats to the system (from Threat Assessment)
(Update) Identify System Vulnerability
Quantify the Probability the Threat can exploit the Vulnerability
Quantify the consequence to the mission should the threat exploit the vulnerability
Quantify the Risk based on probability and consequence
Generate Risk Analysis for each Risk
Update Risk Mitigation Approach (for each Medium and High Risk)
(Update) Develop Risk Mitigation Options
(Update)Perform Cost-Benefit Analysis on each proposed mitigation
Update Summary Risk Matrix
Update Summary Risk Report
Supply Chain Risk Assessment
HW Components Risk Assessment
Generate HW Components List
Check the HW components for existing vulnerability against vulnerabilities database

Assess Supply Chain Risk for Critical HW components
Identify Risk Mitigation
SW Components
Generate SW components list
Check the SW components for the existing vulnerability against vulnerabilities database
Assess Supply Chain Risk for Critical SW components
Identify Risk Mitigation
Coordination of Risk Matrix/Analysis with CA
PDR
Update IAS/PIT Determination Package
Update IAS/PIT Determination Pkg
Peer review IAS/PIT Determination Pkg
Program Office review and coordination (Staff Summary Sheet)
CA Review and Coordination
DAA Coordination
SAF/CIO/A6 Approval
Updated Threat Assessment
STAR
Space Capstone
Air Capstone
Integrated Threat Assessment (From OSI)
Research Other Threats
Continuous Threats Updates from Intel
Update Risk Assessment
Update IA requirements (SRTM)
CA approval of updated IA requirements (SRTM)
Identify non compliant IA controls
(Update) Identify threats to the system (from Threat Assessment)
(Update) Identify System Vulnerability
Quantify the Probability the Threat can exploit the Vulnerability
Quantify the consequence to the mission should the threat exploit the vulnerability
Quantify the Risk based on probability and consequence
Generate Risk Analysis
Update Risk Mitigation Approach (for each Medium and High Risk)
(update) Develop Risk Mitigation Options
(update) Perform Cost-benefit analysis on each proposed mitigation
Update Summary Risk Matrix
Update Summary Risk Report
Supply Chain Risk Assessment
HW Components Risk Assessment
Generate HW Components List
Check the HW components for existing vulnerability against vulnerabilities database
Assess Supply Chain Risk for Critical HW components
Identify Risk Mitigation
SW Components
Generate SW components list
Check the SW components for the existing vulnerability against vulnerabilities database
Assess Supply Chain Risk for Critical SW components
Identify Risk Mitigation
Coordination of Risk Matrix/Analysis with CA
Milestone B
Exit Criteria

Approved IA Requirements by CA
Updated Risk Analysis
Data Flow Diagram
EITDR Registration
Engineering & Manufacturing Development (EMD) Phase
CDR
Update IAS/PIT Determination Package
Update IAS/PIT Determination Pkg
Peer Review IAS/PIT Determination Pkg
Program Office Review and Coordination (Staff Summary Sheet)
CA Review and Coordination
DAA Coordination
SAF/CIO/A6 Approval
Update Threat Assessment
STAR
Space Capstone
Air Capstone
Integrated Threat Assessment (From OSI)
Research Other Threats
Continuous Threats Updates from Intel
Update Date Flow
Update Risk Assessment
Update IA requirements (SRTM)
CA Approval of updated IA requirements (SRTM)
Identify Non Compliant IA Controls
(Update) Identify threats to the system (from Threat Assessment)
(Update) Identify System Vulnerability
Quantify the Probability that the Threat can exploit the Vulnerability
Quantify the consequence to the mission should the threat exploit the vulnerability
Quantify the risk based on probability and consequence
Generate Risk Analysis for each risk
Update Risk Mitigation Approach (for each Medium and High Risk)
(update) Develop Risk Mitigation Options
(update) perform cost-benefit analysis on each proposed mitigation
Updated Summary Risk Matrix
Update Summary Risk Report
Supply Chain Risk Assessment
HW Components Risk Assessment
Generate HW Components List
Check the HW components for existing vulnerability against vulnerabilities database
Assess Supply Chain Risk for Critical HW components
Identify Risk Mitigation
SW Components
Generate SW components list
Check the SW components for the existing vulnerability against vulnerabilities database
Assess Supply Chain Risk for Critical SW components
Identify Risk Mitigation
Coordination of Risk Matrix/Analysis with CA
TRR
IATT
Architecture Analysis
Develop/Refine/Review System Security Architecture Diagram

Develop/Refine/Review Information/Data Flow Diagram
Develop/Review External and Internal interfaces Diagram/Document
Data Flow Analysis
Architecture and Data Flow Review with CA
Updated Threat Assessment
STAR
Space Capstone
Air Capstone
Integrated Threat Assessment (From OSI)
Research Other Threats
Continuous Threats Updates from Intel
Requirements Analysis/Verification
Verify external system/subsystem connection C&A
Analyze the risk associated with external system/subsystem connection
Delineate/Assign IA controls for site C&A
Tailor Validation Procedures
Asses/Verify IA Requirements (SRTM) Compliance and gather compliance artifacts
Coordination of requirements analysis and compliance with CA
Coordination of Requirements analysis and compliance with the program office and User Co
Test/Analysis/Evaluation
Analyze the Test Reports/Results
Perform/Analyze Gold Disk Vulnerability Scan
Perform/Analyze Flow Finder scans (on the applicable CSCIs)
Perform/Analyze Vulnerability Assessment scans by Reina (eEye) Tool (if applicable
Review/Analyze 46th Test Squadron Test Report
Site specific IA controls verification
EMSEC (TEMPEST) Test Results Review
Software Assurance (SWA)
Generate SW Components List
Check the SW components for the existing vulnerability against vulnerabilities datab
Assess Supply Chain Risk for Critical SW components
Update Risk Assessment
Identify Non Compliant IA Controls
(Update) Identify threats to the system (from Threat Assessment)
(Update) Identify System Vulnerability
Quantify the Probability that the Threat can exploit the Vulnerability
Quantify the consequence to the mission should the threat exploit the vulnerability
Quantify the risk based on probability and consequence
Generate Risk Analysis for each risk
Update Risk Mitigation Approach (for each Medium and High Risk)
(update) Develop Risk Mitigation Options
(update) perform cost-benefit analysis on each proposed mitigation
Updated Summary Risk Matrix
Update Summary Risk Report
Supply Chain Risk Assessment
HW Components Risk Assessment
Generate HW Components List
Check the HW components for existing vulnerability against vulnerabilities database
Assess Supply Chain Risk for Critical HW components
Identify Risk Mitigation
SW Components
Generate SW components list

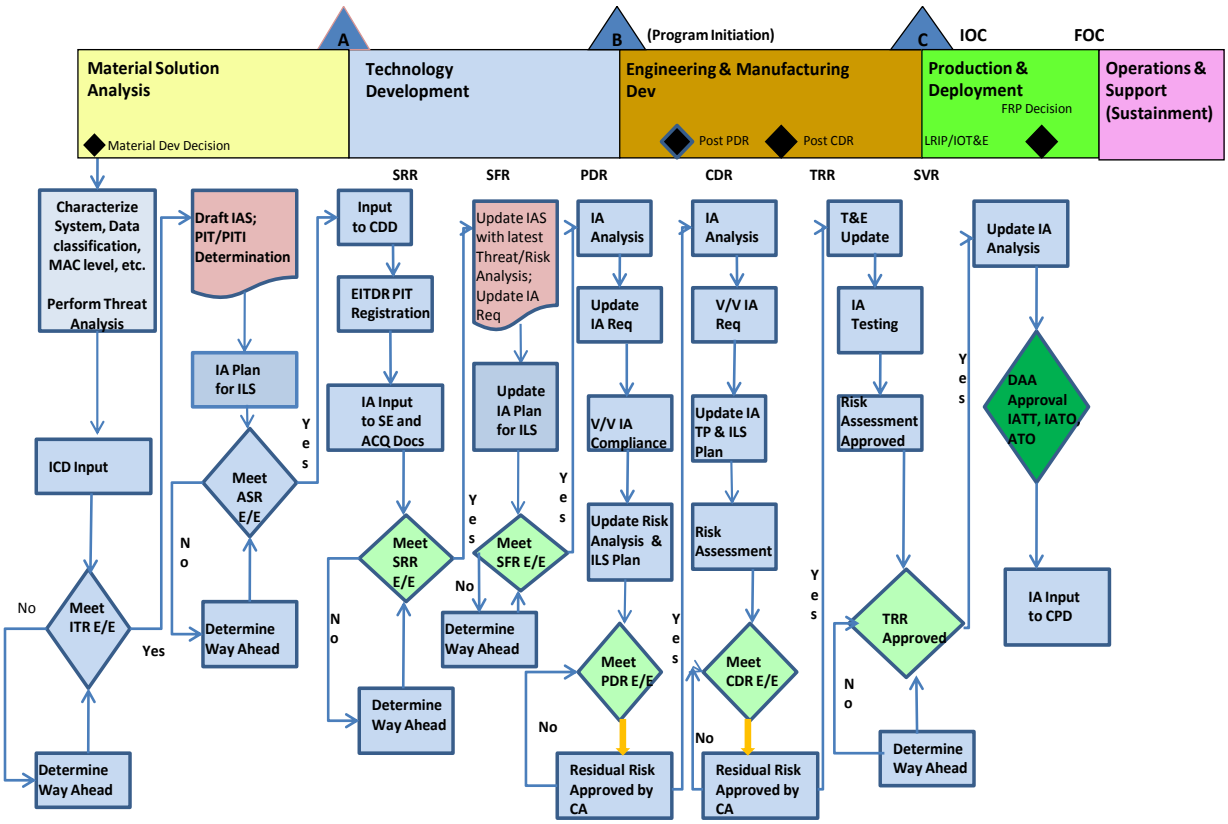
Check the SW components for the existing vulnerability against vulnerabilities database
Assess Supply Chain Risk for Critical SW components
Identify Risk Mitigation
Coordination of Risk Matrix/Analysis with CA
Obtain IATT Approval
Generate IATT Brief
Program Office Review and Coordination of IATT Briefing pkg
User Community Review and coordination of IATT Briefing pkg
Update IATT Brief
Brief the CA
Update IATT Post CA Review
IATT Letter
Draft IATT Letter
Draft Staff Summary Sheet
Program Office Coordination
CA Coordination
EN Coordination
IATO/ATO
Architecture Analysis
Define IA boundary
Review System Security Architecture Diagram
Develop Information/Data Flow Diagram
Data Flow Analysis
Review External and Internal Interfaces Diagram/Document
Review External and Internal Interfaces (Interface Documents)
Verify external system/subsystem Connection C&A
Analyze the risk associated with external system/subsystem documents
Architecture/Data Flow/IA Boundary Review
Review Architecture/Data Flow/IA Boundary with Program Office/Site
Create the briefing
Review the Briefing with PO
Update the Briefing (Post Review with PO)
Review Architecture/ Data Flow/IA Boundary with CA
Review the Briefing with CA (with PO)
Update the Briefing (Post Review with CA)
Develop Updated Threat Assessment Matrix
Review Existing Integrated Threat Assessment
Research Other Threats (Weekly Threat Bulletins, HOTR Research)
Continuous Threats Update from Intel Folks
Generate Updated Threats Assessment Matrix
Develop Threats/Vulnerabilities Mapping Matrix
Identify/Assess the vulnerabilities from the Architecture Analysis
Generate Threats/Vulnerabilities Mapping Matrix
Develop IA Requirements
Perform Initial Risk Assessment
Define IA Requirements (controls) (SRTM)
Define IA Verification procedures
Review Threat/Vulnerabilities matrix and IA Requirements with CA
Review Threat/Vulnerabilities Matrix

Review Initial Risk Assessment
Review IA Requirements and Verification Methods
Update IA Requirements (Post CA Review)
Test/Analysis/Evaluation
Requirements Compliance Verification
Assess/Verify IA Requirements (SRTM) Compliance
Assess/Verify the Site IA Requirements Compliance
Gather artifacts related to the IA requirements compliance
Site Visit/Findings
Review Physical (HW) Architecture
Review Software Architecture (Verify the SW list in operational environment)
Review Operational Environment
Review Interfaces (External and Internal)
Site Visit Finding Report
Develop/Refine/Review system Security Architecture Diagram
Develop/Refine/Review Information/Data Flow Diagram
Develop/Review External and internal interfaces Diagram
Updated Threats Vulnerabilities Analysis Report
Perform Risk Analysis (Threats and Vulnerabilities)
Analyze the Test Reports/Results
Perform/Analyze Gold Disk Vulnerability Scan (if applicable)
Perform/Analyze Flow Finder scans (on the applicable CSCIs)
Site specific IA controls verification
EMSEC (TEMPEST) Test Results Review
Software Assurance (SWA)
Generate SW Components List
Assess the Software Assurance
Risk Assessment
Identify Non Compliant IA Controls
Map the Non Compliant controls to the Threats/Vulnerabilities Matrix
Generate Risk Analysis for each Risk
Quantify the Probability the Threat can exploit the Vulnerability
Quantify the consequence to the mission should the threat exploit the vulnerability
Quantify the Risk based on probability and consequence
Risk Mitigation Approach (for each Medium and High Risk)
Develop Risk Mitigation Options
Perform Cost-Benefit Analysis on each proposed mitigation
Update Summary Risk Matrix
Update Summary Risk Report
Supply Chain Risk Assessment
HW Components Risk Assessment
Generate HW Components List
Check the HW components for existing vulnerability against vulnerabilities database
Assess Supply Chain Risk for Critical HW components
Identify Risk Mitigation
SW Components
Generate SW components list
Check the SW components for the existing vulnerability against vulnerabilities database
Assess Supply Chain Risk for Critical SW components
Identify Risk Mitigation

IA Team Review of Risk Assessment	
Create Risk Assessment Brief	
Review Risk Assessment with IA Team	
Update Risk Assessment and Brief (post review with IA team)	
Risk Assessment Review with CA	
Review Risk Assessment with CA	
Update Risk Assessment and Brief (Post Review with CA)	
System Security Plan (SSP)	
Develop SSP	
Peer Review of SSP	
Update SSP	
DAA Approval	
Staff Summary Sheet Coordination	
Program Office Review and Coordination	
User Community Review and Coordination	
CA Review and Coordination	
DAA Approval/Signatures	
Obtain IATO Approval	
Generate IATO Brief	
Program Office Review and Coordination of AITO Briefing Pkg	
User Community Review and Coordination of AITO Briefing Pkg	
Update IATO Brief	
Brief the CA	
Update IATO Post CA Review	
IATO Letter	
Draft IATO letter	
Draft Staff Summary Sheet	
Program Office Coordination	
CA Coordination	
EN Coordination	
Brief the DAA	
IATO Approval by DAA	

PIT in the Acquisition Process Summary

The below flowchart is a summary of IA within the system engineering acquisition process.



PIT Developmental Systems:
C&A Process

1

1.0 Material Solution Analysis (MSA) Phase

The purpose of this phase is to assess potential Material Solutions and to satisfy the phase-specific entrance criteria for the next program milestone designated by the Milestone Decision Authority (MDA). Entrance into this phase depends upon an approved Initial Capabilities Description resulting from the analysis of current mission performance and an analysis of potential concepts across the DoD, international systems from allies, and cooperative opportunities.

1.1 Initial Threat Assessment

See the PIT Guidebook core section for information on the Threat Assessment.

1.2 PIT Determination Package

The PIT Determination Package will include all related material required for the Certification Authority (CA)/Designated Accrediting Authority (DAA) and/or AFNIC to make an informed decision regarding whether the system qualifies as a PIT. The PIT checklist is utilized to help make the PIT decision. (see section 3 of the core PIT Guidebook)

1.2.1 Approval Process

1.2.1.1 PIT Determination Package without an Information Assurance Strategy (IAS)

The PIT Determination Package as described above is sent to the PIT CA for their review and determination. A meeting with the CA may be required to answer questions regarding information not apparent or missing in the package. If the PIT Determination is approved by the CA, it is forwarded to the PIT DAA for concurrence. The PIT Determination package is then sent to the AF-CA (AFNIC/EV) for their approval representing the AF-DAA.

1.2.1.2 PIT Determination Package as part of an IAS

If an IAS is to be written, then section 8 of the IAS will indicate the PIT process is to be used. The IAS will also include the required artifacts as indicated above including the PIT Determination checklist as appendices. The PIT CA and PIT DAA need to concur on the PIT determination prior to submittal of the IAS. The IAS is ultimately approved by SAF CIO/A6. Once the IAS is approved, then that also constitutes approval as a PIT. Below is the outline for an IAS.

IAS Outline

The IAS is a requirement of the Clinger-Cohen-Act (CCA) per DoDI 5000.2, May 12, 2003, Table E.4.T1. The program engineer or Program Manager (PM) usually develops the IAS early in the program. A shell of the IAS is required at Milestone A, with updated content provided for each successive Milestone. For programs already past Milestone B, but preparing to enter Milestone C, check with the MDA to see if an IAS is required at such a late date. If it is unclear,

then an IAS should be prepared. The PIT CA and PIT DAA approve the IAS initially with SAF/CIO A6 having final authority over the IAS approval. For new programs, approval of the IAS with the required PIT information (as an appendix to the IAS) constitutes approval as a PIT program. This IAS Template is from the Defense Acquisition Guide.

IAS Template

1. **Program Category and Life Cycle Status**: Identify the Acquisition Category of the program. Identify current acquisition life cycle phase and next Milestone decision.
2. **Mission Assurance Category (MAC) and Confidentiality Level**: Identify the system's MAC and Confidentiality Level as specified in the capabilities document in accordance with DoD Instruction 8500.2
3. **System Description**: Provide a high-level overview of the specific system being acquired, including a block diagram that shows major elements/subsystems that make up the system being acquired. Describe at a high level the Information Assurance (IA) technical approach that will secure the system, including any protection to be provided by external systems or infrastructure.
4. **Threat Assessment**: Describe the methodology used to determine threats to the system (such as the System Threat Assessment) and whether IA was included in the overall weapon system assessment.
5. **Risk Assessment**: Describe the program's planned regimen of risk assessments, including a summary of how any completed risk assessments were conducted.
6. **Information Assurance Requirements**: Describe the program's methodology used for addressing IA requirements early in the acquisition lifecycle. Identify the applicable sets of Baseline IA Controls from DoDI 8500.2 that will be implemented. Specify whether any specific IA requirements are identified in the approved governing requirements documents (e.g. CRD, ICD, CDD, CPD). Describe how IA requirements implementation costs (including costs associated with Certification and Accreditation (C&A) activities) are included and visible in the overall program budget.
7. **Acquisition Strategy**: Provide a summary of how IA is addressed in the program's overall acquisition strategy document. Describe how the Request for Proposal (RFP) for the System Development and Demonstration Phase contract was, or will be, constructed to include IA requirements in both the operational and system performance specifications, and integrated into the system design, engineering, and testing. In addition, describe how the RFP communicates the requirement for personnel that are trained, and appropriately certified in accordance with DoDD 8570.1, in IA. Address whether the program will be purchasing commercial off-the-shelf IA or IA-Enabled products, and the program's means for verifying that the "National Policy Governing the Acquisition of IA and IA-enabled Information Technology Product" will be followed.
8. **C&A**: Identify the specific C&A process to be employed (e.g. DoD IA C&A Process (DIACAP) or PIT process). Provide the name, title, and organization of the DAA, CA, and User representative. If the program is pursuing and evolutionary acquisition approach (spiral or incremental development), describe how each increment will be

subjected to the C&A process. Provide a timeline graphic depicting the target initiation and completion dates for the C&A process, highlighting the issuance of IATT, IATO, and ATOs. Normally, it is expected that an ATO will be issued prior to Operational Test and Evaluation (OT&E). If the C&A process has started, identify significant activity completed and whether an ATO or IATO was issued. If requesting a PIT Determination as part of the IAS, provide a PIT Determination Package per the PIT Guidebook.

9. **IA Testing**: Discuss how IA testing has been integrated into the program's test and evaluation planning, and incorporated into program testing documentation, such as the Test and Engineering Master Plan (TEMP).
10. **IA Shortfalls**: Identify any significant IA shortfalls, and proposed solutions and/or mitigation strategies. Specify the impact of failure to resolve any shortfall in terms of program resources and schedule, inability to achieve threshold performance, and system or warfighter vulnerability. If the solution to an identified shortfall lies outside the control of the program office, provide a recommendation identifying the organization with the responsibility and authority to address the shortfall. If applicable, identify any Acquisition Decision Memoranda that cite IA issues.
11. **Policy/Directives**: List the primary policy guidance employed by the program in preparing and executing the Acquisition IAS, including the DoD 8500 series, and DoD component, Major Command/Systems Command, or program-specific guidance, as applicable.
12. **Relevant Associated Program Documents**: Provide statement that this version of the Acquisition IAS is reflective of the program requirement and capabilities documents dated _____.
13. **Point of Contact**: Provide the name and contact information for the program management office individual responsible for the Acquisition IAS document.

1.2.2 Initial PIT IA Boundary

The initial IA boundary should be drawn which shows what elements of the weapon system are to be included in the IA analysis. Examples of these elements may be the aircraft, maintenance system, training system, or data loading system.

1.3 Milestone A (MS-A) Criteria

The conclusion of MS-A leads to the Technology Development Phase. An Alternate System Review is required along with the Technology Development Strategy. This should include any IA requirements which are considered to be high risk. This would allow for technology to be developed to mitigate the risk.

2.0 Technology Development (TD) Phase

The TD Phase is used to reduce technology risk, determine and mature appropriate set of technologies to integrate into a full system. Critical technologies are demonstrated on prototypes and the preliminary design review is usually accomplished.

2.1 Determine IA Requirements for System Requirements Document (SRD)/RFP

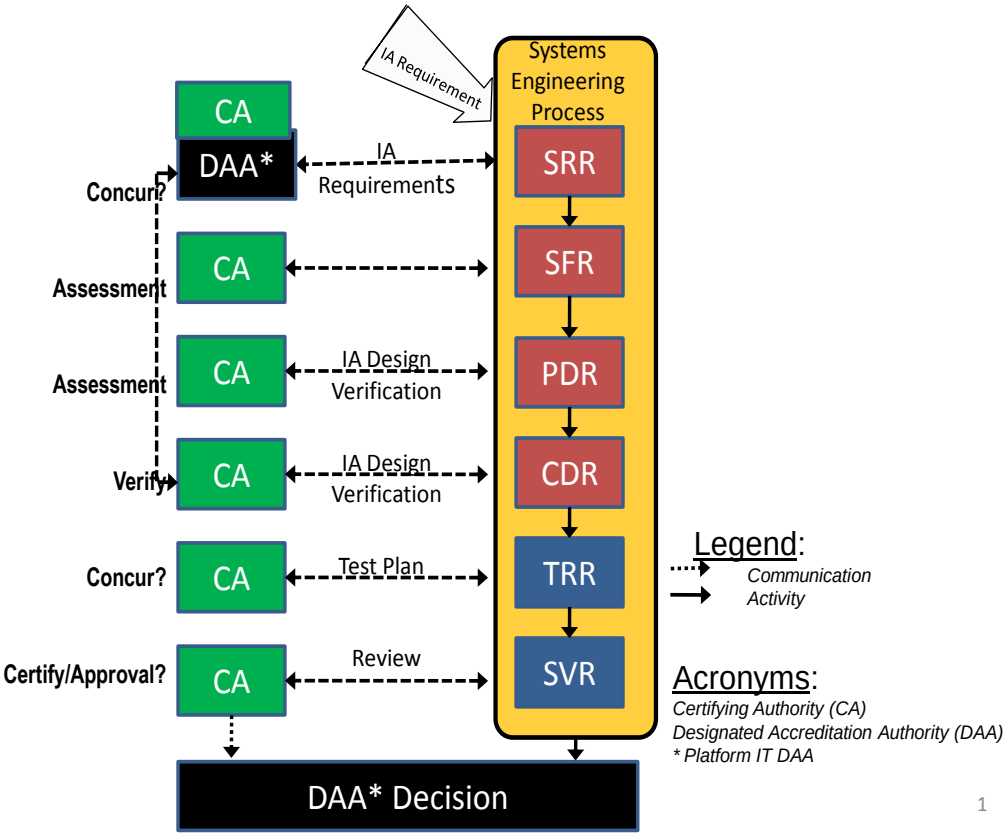
2.1.1 Tailored System Requirements Traceability Matrix (SRTM)

The IA requirements for the program are generally derived from DoDI 8500.2 and/or National Institute of Standards (NIST) Special Publication (SP) 800-53. The IA requirements from DODI 8500.2 were originally designed for IT systems. A PIT system does not have to follow the 8500.2 controls exactly as written. The system under consideration may have different requirements based on the threats which exist and its vulnerability. It is expected that specific controls may be derived for the system. The 8500.2 and/or NIST controls are a good starting point to derive the majority of the IA requirements. Some of the controls will not be applicable; others may apply but will not be utilized due to system requirements, while other controls are tailored to meet the system requirements. A Platform Information Technology Interconnection (PITI) system is required to follow the DODI 8500.2 controls as written or be waivered due to other program considerations.

2.1.2 IA Requirements Approval by the CA

The IA requirements derived for the program form the basis of the IA program and need to be approved by the CA. The CA will require the program description, IA boundary, and information and data flow to help with their determination. The baseline requirements are established early in the program and then revised as part of the System Requirements Review (SRR) design review. Once approved for the SRR, the IA requirements need to be tracked throughout the design and testing phases of the program. See the below flowchart for the system engineering approval by the CA and DAA for all phases of acquisition.

IA Systems Engineering Approach



1

2.2 SRR Entrance Criteria

- IA approach understood by both the contractor and the Government
- Risk management approach understood by all concerned parties
- IPT formed if not done previously
- Key technology information that affects IA understood
- IA requirements traceable to the MSA phase

2.3 SRR Exit Criteria

- Government and contractor agree on the IA requirements
- CA approves IA requirements
- Design constraints that affect IA identified
- Define information functions, flows, and values
- Identify IA impacts on the system functional architecture
- Review and update threats and weaknesses

2.4 IA Stakeholders

It is important all stakeholders in the program collaborate in the conduct of the IA program. The stakeholders include the CA, DAA, PM, IA engineer, users, Test and Evaluation (T&E) community, and laboratories as needed. Some programs may require a written Memorandum of Agreement between DAAs. The stakeholders group will be vitally important when deciding the IA Risk Assessment and any mitigation required.

2.5 INTEL Threat Assessment

The program threat assessment accomplished during the MSA Phase should be updated with the latest information. This information may sometimes alter the IA posture.

2.6 Source Selection Plan

The Source Selection Plan should include the language for the IA requirements in the SRD, Statement of Objective or Statement of Work and the Sections L and M of the RFP.

2.7 System Functional Review (SFR)

The primary purpose of the SFR is to analyze the progress made to date and whether the system can proceed to the PDR. The proposed system should be fully decomposed and defined in the functional baseline. The system performance is decomposed and traced to lower level subsystem hardware and software.

2.7.1 SFR Entrance Criteria

- Successful completion of the Preliminary Design Review (PDR) with CA approval of the IA requirements
- Trace the IA requirements back to the MSA and TD phases

2.7.2 SFR Exit Criteria

- The IA needs for the security function within the system are defined
- IA design constraints identified
- Define the information functions (activity), flows (data flow diagram) and values
- Refine the IA input to the system functional architecture

2.8 PDR

The PDR is normally the first major design review of the proposed solution by the contractor.

2.8.1 Entrance Criteria

- The IA SRTM resulting from the SRR tracks to all IA requirements and has been approved by the PIT CA and PIT DAA as necessary.
- System engineering documentation has been updated to include the IA requirements.

2.8.2 Exit Criteria

- A preliminary IA Risk Assessment matrix was completed which traces to the SRTM established at the SRR
- The PIT CA concurs with the IA position resulting from the PDR
- System Engineering documentation has been updated to reflect the preliminary IA design allocation including a preliminary TEMP

2.9 Outputs of the Technology Phase

IA plays a role in the following documents: Systems Engineering Plan (SEP), TEMP, Capabilities Description Document (CDD), and the Information Security Plan (ISP).

2.9.1 Initial IA Risk Assessment

The initial Risk Assessment should be accomplished during the PDR if held during this phase. Each IA requirement agreed to at the SRR should be addressed during the design review. Those requirements not considered to be low risk as a result of the design review need to be reviewed with the CA.

2.9.2 Enterprise Information Technology Data Repository (EITDR) Registration

The weapon system needs to be registered in the EITDR regardless if it is considered PIT or PITI. For PIT, there are approximately twenty questions to answer. Check with your local Chief Information Officer (CIO) for guidance regarding registration.

2.10 Milestone B Criteria

To exit from the Technology Development Phase into the Engineering and Manufacturing Development (EMD) Phase requires the following actions:

- CCA compliance, includes IAS and PIT Determination
- Draft IA input to the CDD with Key Performance Parameters addressed
- Identification of High Risk Technologies resolved
- System Performance Specification baselined
- Appropriate documentation developed (IA inputs to SEP, TEMP, ISP, and Program Protection Plan)
- Successful PDR if held during this phase
- Registered in EITDR

3.0 EMD Phase

The EMD Phase consists of two parts:

- Integrated System Design
- System Capability and Manufacturing Process Demonstration

3.1 Milestone C (MS-C) Criteria (end of EMD, start of Production & Deployment)

Tasks that must be accomplished during EMD prior to a MS-C decision are:

- Update previous documentation
- Ensure CCA compliance with the CIO
- Update threat assessment
- Ensure the IA requirements are current
- IA Risk Assessment accomplished and proper C&A accomplished for the system

3.2 Critical Design Review (CDR)

Upon completion of a successful CDR, the design is finalized and the development of both hardware and software.

3.2.1 Entrance Criteria

- Successful completion of the PDR with the PIT CA concurring with the IA posture and the SRTM updated to reflect the IA requirements

- System engineering documentation has been updated to include the IA requirements

3.2.2 Exit Criteria

- IA requirements are traced back to the requirements determined at the MSA and TD phases
- All IA requirements are addressed and implementation of them is reflected in the physical design or operation of the system
- Interfaces/protocols are defined
- Architecture is analyzed against the IA requirements
- Each configuration item reflects the IA requirements
- Security operation of the system is agreed to by the end user and the program office
- Life-cycle approach finalized and test matrix updated
- Risk management plan is updated to reflect latest threats and weaknesses
- Mitigation techniques for risks not considered low are agreed to by the IPT, contractor, and approved by the CA

3.3 Test Readiness Review (TRR)

The TRR is to evaluate if the system is mature enough to enter formal testing.

3.3.1 TRR Entrance Criteria

- All IA requirements must be associated with the test matrix
- Each IA requirement traceable back to the original requirement at SRR

3.3.2 TRR Exit Criteria

- Each IA requirement is addressed by Analysis, Inspection, Demonstration, or Test in the test documentation
- Any IA requirement not considered low risk is given special consideration to either prove it is low during testing or procedures are developed to mitigate the risk

3.4 System Verification Review (SVR)

The SVR is synonymous with the old terminology Functional Configuration Audit. The review is to ensure the system can proceed into production and is normally held in conjunction with the Production Readiness Review (PRR).

3.4.1 SVR Entrance Criteria

- Successful TRR
- IA is documented in the Configuration and Product Specifications

3.4.2 SVR Exit Criteria

- IA is addressed in the Capabilities Product Document.
- IA Risk Management matrix is complete
- PIT DAA issues operational decision (IATO, ATO, DATO)

3.5 PRR

Normally at PRR all IA issues have been addressed. The only issue would be if an IA requirement is driving a special design that is complex and very risky. In that case, a decision should be made regarding whether the IA mitigation is warranted.

3.6 Special Documentation and Test Procedures for Acquisition Programs

3.6.1 System Security Plan (SSP)

An SSP that is a major document related to IA Documentation. The SSP is required prior to Initial Operational Capability of the system. The purpose of this document is to specify the assumptions, objectives, and set the baseline for the definition of the security requirements for the particular program based on applicable laws, policies, and regulations. The document blends multiple security policies necessary to protect the system resources (equipment, personnel, data, etc.) from denial of service, damage, tampering, espionage, fraud, misappropriation, misuse, unauthorized modification, and unauthorized disclosure. The SSP should put into effect the set of rules and practices regulating the management, use, protection, distribution, creation, destruction, and manipulation of data entrusted to the program users and personnel who maintain, administer, and operate all the elements, subsystems, and interfaces for the program. The following is an outline of the information that should be included in the SSP. The content is important not the format. The SSP works with the IA risk assessment and some of the mitigations maybe specified in the SSP.

1.0 Introduction
- 1.1 Purpose
- 1.2 Scope
- 1.3 Roles and Responsibilities
  - 1.3.1 Certifying Authority (CA)
  - 1.3.2 Designated Accrediting Authority (DAA)
  - 1.3.3 Information Assurance Manager (IAM)
  - 1.3.4 Information Assurance Officer (IAO)

2.0 System Description/Concept of Operations (CONOPS)
- 2.1 Hardware
- 2.2 Software

3.0 Facility Description
- 3.1 Physical Security

4.0 Accreditation Boundary
5.0 System /Data Criticality
6.0 Configuration Management (CM)
7.0 System Security
    7.1 Governing Security Requisites
    7.2 Accountability
    7.3 Data Security Requirements
        7.3.1 Availability
        7.3.2 Integrity
            7.3.2.1 Data Integrity
            7.3.2.2 System Integrity
        7.3.3 Confidentiality
    7.4 Method of Access Control
        7.4.1 Authorization
        7.4.2 Access
        7.4.3 User Accounts
        7.4.4 Group Accounts
        7.4.5 System Administrators and User Privileges
        7.4.6 Passwords
        7.4.7 Password Protection
    7.5 Audit
        7.5.1 Events and Information to be Audited
        7.5.2 Automated or Manual Audit
        7.5.3 Retention of Audit Record
        7.5.4 Audit Review
        7.5.5 Protection of Audit Files
    7.6 System Security Requirements
        7.6.1 Unattended Workstations/Time-Out Policy
        7.6.2 Internet Access
        7.6.3 Port Security
        7.6.4 Antivirus Software
8.0 Communications Security (COMSEC)
9.0 Physical Security/Resource Protection
    9.1 Logical Resource Protection
    9.2 Security Clearances
    9.3 Hardware/Firmware Controls
        9.3.1 Maintenance
        9.3.2 Software Maintenance
10.0 Contingency/Disaster Planning

3.6.2 Life-Cycle Sustainment for IA (continuous monitoring)

3.6.2.1 Role of the Configuration Control Board (CCB)

The CCB maintains control of the configuration of the product. Changes to the established baseline must be approved by the CCB. Any change to the hardware or software of the product must be evaluated for impacts to IA. Someone with IA knowledge and interest should be a member of the CCB. If a change impacts IA, then the CCB must take this into consideration prior to approving the change.

3.6.2.2 Periodic Re-Certification and Accreditation

The PIT DAA will determine when a system should be revisited to ensure it is still meeting its IA requirements and C&A. A no-notice inspection may be required on a schedule determined by the DAA depending on the risk nature of the program. DIACAP give guidelines for systems certified and accredited by the DIACAP process. These may be used as guidance for PIT.

3.6.3 Test and Evaluation of Acquisition Systems

3.6.3.1 Air Force Operation Test and Evaluation Center (AFOTEC)

AFOTEC's role:

AFOTEC evaluates IA as part of an OT&E to determine operational effectiveness, suitability, and overall mission capability. Effectiveness and suitability of the system's IA measures are reported in relation to operational impact and Mission Assurance. The IA evaluation reveals the capabilities and limitations of the system's IA posture and the effectiveness and suitability in the presence of realistic Information Operations threats and countermeasures.

During DT (prior to IATO or ATO):

AFOTEC collaborates with external agencies ensuring IA is assessed as early as possible in the acquisition cycle to determine vulnerabilities, risks, and mitigating actions.

AFOTEC's early and continuous influence through Integrated Development Test/Operational Test (IDT/OT) maximizes the availability of data and obtains operationally realistic data during DT. IDT/OT facilitates the sharing of common operationally relevant data along with achieving an overall reduction in time and cost for OT and the reduction in risk during OT activities and events.

AFOTEC participates in IDT/OT and uses resultant IA data to assess or evaluate the system and identify significant IA residual risks. Assessing IA as part of an Operational Assessment or an Early Operational Assessment focuses on the potential impact of the system's IA attributes on

mission assurance and provides insight into progress toward operational effectiveness, suitability, and system readiness for OT&E.

AFOTEC is not a required participant in system C&A, but may request to observe C&A activities. AFOTEC requires insight into system design and C&A information such as IA Strategy, Plan of Action and Milestones (POA&M), Vulnerability Management Plan, etc. (Complete AFOTEC Document Listing in Appendix I).

AFOTEC incorporates Director, OT&E IA testing procedures, plans the OT&E events and coordinates the applicable OT&E vulnerability and penetration testing that will be executed in the operational environment.

AFOTEC reviews the PIT designation approval and PIT C&A package. AFOTEC receives the approved IATO or ATO prior to Operational Test Readiness Review (required prior to start of OT&E).

During OT&E:

AFOTEC works with the Integrated Test Team to develop an IA test plan based on the PIT designation package.

AFOTEC employs the same OT of IA methodology for PIT as for GIG-enabled systems. Test methods, such as interview, documentation review and technical testing are used to assess all applicable IA controls as determined in the PIT documentation. The AFOTEC measures are still based on the SRR for the tailored DoDI 8500.2 IA controls provided by the PIT IPT.

Comprehensive IA assessment is an integral part of every OT program. Our IA assessment will address operational, management and technical aspects of the system design and the acquisition program.

AFOTEC, in conjunction with any external test agencies, will conduct the IA testing either before or during scheduled OT&E events. Upon completion, AFOTEC IA personnel will generate a report detailing the findings of the IA testing.

OT&E technical (penetration) assessments seek to identify vulnerabilities internal to the system and through external connections such as via PITI, PIT-to-PIT or RF links.

Below is a list of documents typically reviewed by AFOTEC to evaluate weapon systems for IA compliance.

Typical Documents Reviewed by AFOTEC

Document Title	Doc Date	Reviewed	Remarks/Issues
Sample Security Document	DD/MM/YY	Yes/No	Draft/Completed/Signed/Unsigned
ATO Memorandum			
Configuration Management Plan			
Continuity of Operations Plan			
Disaster Recovery Plan			
Hardware Baseline Table			
IAM Memorandum			
IATO Memorandum			
IATT Memorandum			
Incident Response Plan			
Information Assurance Strategy			
Information Support Plan			
Information System Security Plan			
Interim Contractor Support Plan			
Lifecycle Management Plan			
Operational Concept			
Operations Security Plan			
POA&M			
Ports, Protocols, and Procedures			
Security Concept of Operations			
Service Level Agreement			
Software Baseline Table			
Software Development Plan			
System Engineering Plan			
System Identification Profile			
System Installation Procedures			
Vulnerability Management Plan			

3.6.3.2 Air Force System Interoperability Test (AFSIT)

The AFSIT organization tests Air Force Systems that deploy Tactical Data Links for standards conformance (Mil-STD-6016, 6011, 3011, 6017, 6040, etc.). The test is conducted in a closed network lab so no IATT, IATO or ATO is required. AFSIT does their testing prior to JITC performing their tests. AFSIT does not test for Information Assurance. A system that fails AFSIT testing will not be tested by JTIC.

3.6.3.3 Joint Interoperability Test Command (JITC)

The JITC is part of the Defense Information Systems Agency (DISA). JITC tests and evaluates information technology to ensure interoperability. JITC is the sole DoD joint interoperability

certification authority per the Chairman Joint Chiefs of Staff Instruction 6212.01E. JITC also has an IA team that operates on a fee-for-service basis that can support IA testing to satisfy IA requirements and provide artifacts to the PIT CA and PIT DAA for use in PIT C&A.

3.6.4 Special Testing Concerns

3.6.4.1 Emissions Security also known as TEMPEST

TEMPEST is an unclassified term referring to testing of compromising emanations. Compromising emanations are unintentional signals that, if intercepted and analyzed, could disclose classified information when they are transmitted, received, handled, or otherwise processed by any information processing equipment. TEMPEST is one of the Confidentiality Controls. There are generally questions regarding TEMPEST, which is the reason this control is singled-out for discussion. For weapon systems, if classified or sensitive information is being processed or displayed, then TEMPEST testing is required. For strictly unclassified weapon systems, TEMPEST testing is not required unless dictated by a test agency, such as AFOTEC or by higher headquarters. TEMPEST testing is generally accomplished by the Air Force Certified TEMPEST Technical Authority.

3.6.4.2 Software Testing

Software Quality is another IA requirement that is singled-out for special attention due to the increased use of 3rd party software in PIT systems.

3.6.4.2.1 Pedigree

IA is concerned with the pedigree of any software utilized on the weapon system. Software developed by a cleared contractor for weapon system is the least risky. Software (freeware) downloaded over the internet, where the author is from a foreign country might be considered the riskiest. The following is a checklist to help judge the risk involved in utilizing software from commercial sources, 3rd party software and software not specifically written for the application. In this document we address the idea of qualifying previously unqualified software vendors. By addressing the sourcing and answering a series of questions, an analysis can be done to create a Risk/threat score. This Risk/threat score can be used to help guide in the selection and qualification of a software vendor. This score will help quantify the potential risk of the products generated by the previously unqualified software vendor.

Previously Unqualified Software Vendor Sourcing:

Software Vendor Assurance issues include not only unintentional vulnerabilities, but intentional vulnerabilities. We must determine if certain sources are unacceptable and must not be considered.

For example, many US organizations follow the US regulations regarding countries of concern:

- Nation states named in the US State Department's list of state sponsors of terrorism. http://www.state.gov
- Nation states that are named in the US international trafficking in arms regulation (ITAR, Part 126), for which exports and sales are prohibited as a matter of US national policy.
- Nation states, against which the US maintains an arms embargo (ITAR, Part 126).
- Nation states named in the US national intelligence estimate, "Cyber Threats to the US Information Infrastructure" (available from the National Intelligence Board).

Acquirers may also determine that certain sources are preferred, because they have less risk of including intentional vulnerabilities. For example, some US organizations may determine that countries with historically strong security ties to the US have less risk (such as member states of NATO, nation-states with bilateral security treaties with the US, and Australia, Canada, and New Zealand).

Note that identifying suppliers by country is by no means sufficient to address assurance. Many suppliers reside globally, many developers have citizenships differing from the supplier organization, and mere citizenship of a component developer does not guarantee assurance. In addition, products and services often contain elements acquired elsewhere, and the pedigree of the component may or may not be available. This does *not* imply that "domestic is good, foreign is bad." In many cases, avoiding foreign suppliers will eliminate all of the best suppliers of components, a result to be avoided. Instead, rigor must be put in place to identify and counter potential risks.

In many cases, the Program Manager and the Systems Engineer generally lead the identification of potential suppliers, based on system requirements and market research. At least some of these potential suppliers are typically previously unqualified suppliers (including those who are small or new to the market).

Qualification Questions:

The follow questions have been identified as key to creating a Risk/threat score. Request you carefully and verbosely answer the following questions.

Return your answers to the program office who will then forward your comments to the Information Assurance personnel for analysis, scoring, and issuing a Risk/threat score.

Questions:

1. Facility location
2. Company history
3. Years of operation
4. Nationality of owners
5. Nationality of workers

6. Foreign business affiliations
7. Clearance level of facility
8. Clearance levels of employees
9. Other defense work done for government
10. Is all work done in house? Is any outsourced and, if so, to whom?
11. Is the program going to be turned over to the government?
12. What other programs/organizations/companies/DoD use this software?
13. What other similar systems have been created for DoD?
14. Any government or third-party testing completed (ex JTIC)?
15. What programming language is used?
16. What design standards and processes were followed?
17. What are the safeguards against malicious code?
18. Who is this software licensed to?
19. Who maintains/supports or is it outsourced?
20. Do you have CMMI SEI certifications?
21. Is mobile code used in this software?
22. Any outside code used (public domain, shareware…etc.)?

3.6.4.2.2 Static Code Analysis

Static code analysis is the analysis of software that is performed without actually executing programs built from that software. In most cases the analysis is performed on some version of the source code and in other cases the analysis is performed on the object code. The analysis performed by tools varies from those that only consider the behavior of individual statements and declarations, to those that include the complete source code of a program in their analysis. Uses of the information obtained from the analysis vary from highlighting possible coding errors to formal methods that mathematically prove properties about a given program.

Advantages

- Can find weaknesses in the code at the exact location
- Relatively fast if automated tools are used
- Automated tools can scan the entire code base
- Automated tools can provide mitigations recommendations
- Permits weaknesses to be found early

Limitations

- Automated tools do not support all programming languages
- Automated tools produce false positives and false negatives
- Automated tools can produce a false sense of security
- Does not find vulnerabilities introduced in the runtime environment

3.6.4.2.3 Dynamic Code Analysis

Dynamic code analysis is the testing and evaluation of a software program by executing data in real-time. The objective is to find errors in a program while it is running, rather than by repeatedly examining the code offline. IA is interested in ensuring that the software functions as intended and there is no malicious or hidden code embedded in the software that could disrupt the mission or reveal classified information to those without a need to know.

Advantages

- Identifies vulnerabilities in a runtime environment
- Automated tools provide flexibility on what to scan for
- Allows for analysis of application in which you do not have access to the actual code
- Identifies vulnerabilities that might have been false negatives in the static code analysis
- Validates static code analysis findings
- Can be conducted against any application

Limitations

- Automated tools provide a false sense of security
- Automated tools produce false positives and false negatives
- Automated tools are only as good as the rules used to scan with
- Lack of trained personnel familiar with dynamic code analysis
- Difficult to trace the vulnerability back to the exact location in the code

3.6.5 Air Worthiness Considerations

IA plays a role in the Air Worthiness of a system. Paragraph 15.3.3.4 of MIL-HDBK-516B, Airworthiness Certification Criteria, states "Verify that all data or communications are secure against unwanted intrusions and that security techniques used are implemented safely." In other words, security requirements have been applied to the processing architecture to protect safety critical functions and included in any safety-related analysis/testing. Verification is by inspection of specifications and traceability of security requirements along with test results.

Appendix D

Industrial Control Systems (ICS) Systems Designated as Platform Information Technology (PIT)

Civil Engineering (CE) Platform Information Technology (PIT)
Industrial Control Systems (ICS)

Purpose. This Appendix provides general guidance for Air Force (AF) CE and Information Assurance (IA) managers of CE ICS. This Guide does not override any mandatory policy and guidance outlined in AF Instructions, Engineering Technical Letters (ETL), and higher headquarters memorandums.

Background. ICS is a general term that includes several types of control systems including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as skid-mounted or panel-mounted Programmable Logic Controllers (PLC) often found in the industrial sector and critical infrastructure. ICSs are typically used in infrastructure/utility/industrial systems such as electrical, water and wastewater, oil and natural gas.

AF CE Real Property of Concern. AF CE real property ICS includes, but is not limited to, the following types of systems:

- SCADA
  - Fuel distribution systems
  - Protective relays
  - Cathodic protection systems
  - Power generation, including renewable systems
  - Natural gas
- Energy management and control systems
- Advanced meter reading/utility, including water metering
- Fire alarm/fire suppression/mass notification
- Utility monitoring and control systems
  - Electrical distribution
  - Generator monitoring
  - Water system controls
  - Natural gas
- Airfield control systems
  - Lighting system controls
  - Aircraft arresting system controls
- Traffic signal controls
  - Vehicle barriers
- CE-maintained Intrusion Detection Systems

The above ICSs may be composed of all points, devices, control panels, means of connectivity, software, controllers, and computer-monitoring workstations or servers.

Requirements. AF CD will follow the mandatory guidance and criteria outlined in ETL 09-11. This ETL can be found at http://www.wbdg.org/ccb/AF/AFETL/etl_09_11.pdf. There you will

find technical guidance and criteria for IA of CE ICS. This ETL applies to all ICSs that utilize any means of connectivity to monitor and control industrial processes that includes SCADA, DCS, and other control system configurations such as PLC's, that are often found in industrial equipment and critical infrastructures.

AF CE ICS Points of Contact.

ICS Program Manager: HQ AFCESA/CEOA

ICS PIT Certifying Authority: HQ AFCESA/CEO

ICS PIT Designated Accrediting Authority: HQ USAF/A7C-2

Please contact the HQ AFCESA Reach-back Center for assistance.

DSN: 312-523-6995
Commercial: (850) 283-6995
Toll Free: 888-AFCESA1
NIPR E-mail: AFCESAR@tyndall.af.mil
SIPR E-mail: AFCESA@aetc.af.smil.mil

ICS Packages Community of Practice:
https://afkm.wpafb.af.mil/community/views/home.aspx?Filter=23164

Appendix E

Medical Systems Designated as PIT

AIR FORCE MEDICIAL SERVICE

PLATFORM INFORMATION TECHNOLOGY

Air Force Medical Service

Information Assurance Division

(AFMSA/SG6S)

Falls Church, Virginia

MEDICAL PLATFORM INFORMATION TECHNOLOGY (PIT)

1. Purpose

This appendix is a guide intended to bring a common understanding of Information Assurance requirements for Medical PIT for Program Managers (PM) and Use Representatives. It provides examples and describes the process method for obtaining a statement of exemption from the Certification & Accreditation (C&A) process for Information Technology (IT) systems and IT components defined as Medical PIT.

2. Background

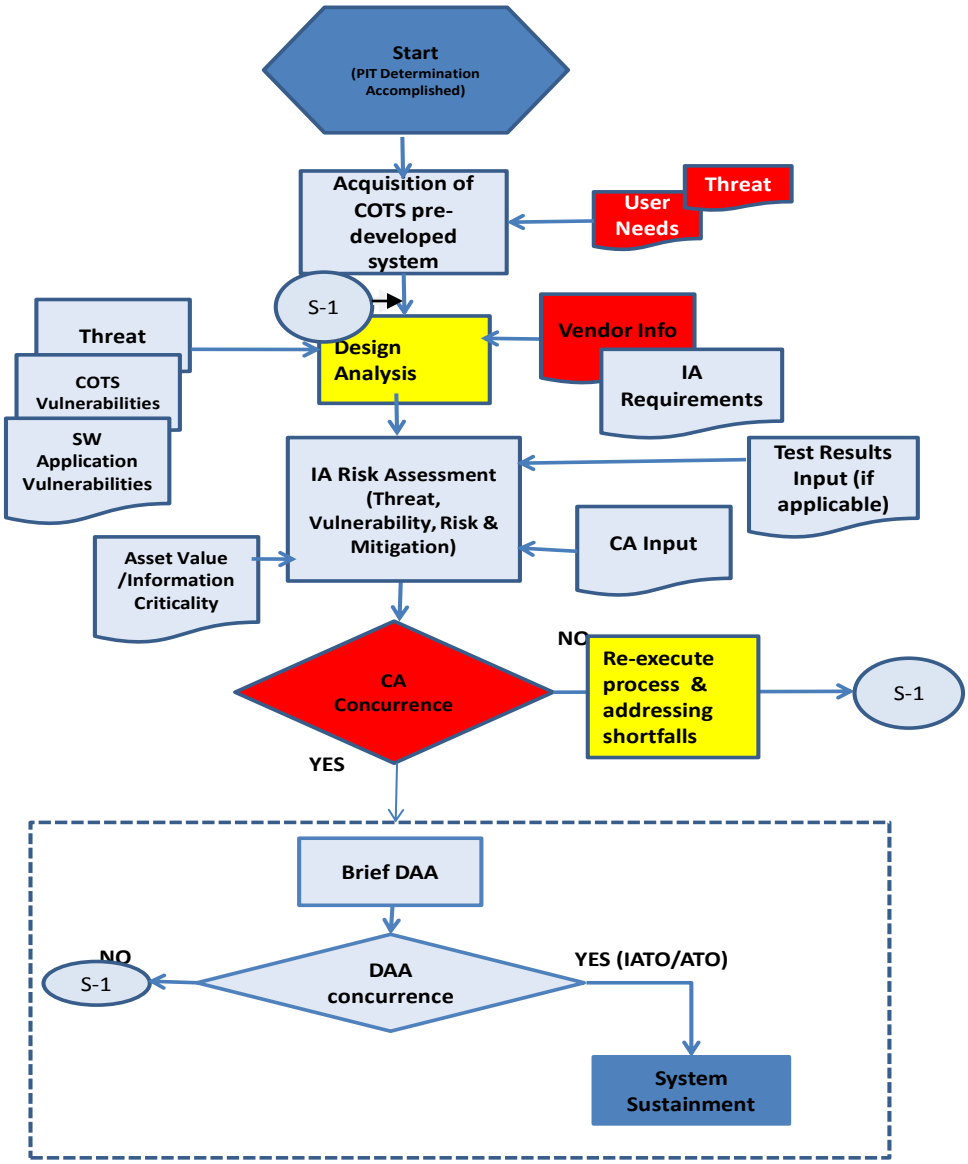
PMs are responsible for ensuring sufficient IA is incorporated into their systems whether or not the C&A process is required. Even under a designation of Medical PIT, PMs shall implement the maximum amount of IA consistent with the special-purpose mission preformed by the Medical PIT.

The IA Controls provided in DoDI 8500.2, Information Assurance Implementation, apply to the definition, configuration, operation, interconnection, and disposal of DoD information systems. They form a management framework for the allocation, monitoring, and regulation of IA resources that is consistent with Federal guidance provided in the Office of Management and Budget Circular A-130, Management of Federal Information Resources. The PM shall ensure IA requirements are managed and implemented throughout the PIT's lifecycle.

Certification Authority (CA) and Designated Accrediting Authority (DAA) Assignment:
AFMSA/SG6 has been delegated the CA for all Air Force Medical Services Automated IS. The Commander, Air Force Medical Support Agency (AFMSA/CC) has been appointed the DAA for all Air Force Medical Services Automated IS.

3. Medical Devices as Commercial-off-the-Shelf (COTS) Systems

Medical devices are considered to be PIT and are to follow the core elements of the PIT Guidebook (sections 1 thru 11). In most cases, the medical PIT is COTS equipment and follows the below COTS/GOTS/MOTS flowchart.



COTS/GOTS/MOTS Flowchart

3.1 Design Analysis

The technical aspect of section 2.3 of the core PIT Guidebook should be adapted as necessary for Medical Systems.

3.2 IA Risk Assessment

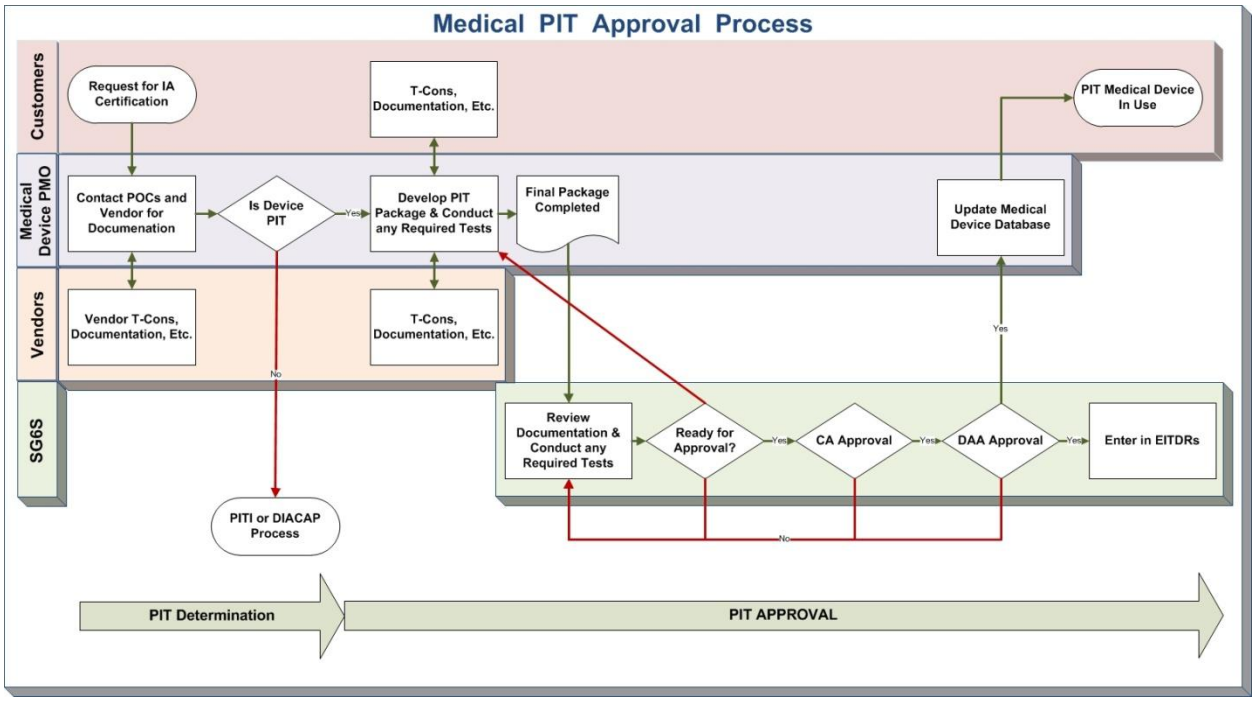
Section 6 of the core IA Guidebook details the risk methodology that is to be used by all PIT systems. Medical systems should adapt this methodology to determine the risk associated with medical devices.

4. Medical Devices Connection to the Global Information Grid (GIG)

In many cases, the Medical PIT device is connected to the GIG via an Intermediate Networked System that is considered to be a PIT Interconnection. Refer to Appendix F for more information on what is considered to be a PIT Interconnection.

5. Medical PIT Approval Process

5.1 Approval Process Flowchart



5.2 Actions Required by PMs for PIT

The Surgeon General (SG) PIT CA and the SG PIT DAA established the following procedure for Medical Devices to obtain a PIT Determination indicating that an IT system or IT component is PIT. Both the SG PIT CA and SG PIT DAA will evaluate the IT with respect of the definition of PIT, and the final determination statement will be issued by the SG PIT DAA in the form of a PIT IT Approval Letter.

AFMOA/SGALE COTS Medical Device Information Security (INFOSEC) Program Office will be the PM providing sponsorship for all Medical Device request. To initiate the official

determination process, User Representatives must submit the following information to AFMOA/SGALE:

1. Vendor Point of Contact.
2. Identification of the IT system or IT component, including its Name, Acronym, and Version Number.
3. Describe the IT system or IT component and its special-purpose mission. In addition to a brief textural description, include a high-level block diagram of the system. For systems with multiple variants, additional diagram may be requested.

Note: AFMOA/SGALE will review all requests to see if another approved device can meet the requirement of the User Representative.

AFMOA/SGALE will provide SG6 the following:

1. Completed PIT Determination Checklist.
2. Description of the IT system or IT component. In addition to a brief textural description, include a high-level block diagram of the system. The diagram must allow the CA and DAA to clearly understand and identify the system's hardware, software, and other components, as well as any interconnection with other systems, networks, or IT. For systems with multiple variants, additional diagram must be submitted describing the variants.
3. Justification for requesting exemption from C&A, to include rationale for classification of the IT system or IT component as Platform IT.
4. Assurance of IA and Risk Management (Section 6 of the core IA PIT Guidebook)
5. Additional supporting documentation if applicable (MDS2, IPV6 compliance, Operational Manuals, etc.).
6. Evaluation request to determine if the IT system or IT component is PIT.
7. Obtain C&A approval.

AFMOA /SGALE will evaluate the User Representative and vendor requests, to ensure the Medical PIT can be used enterprise wide. AFMOA /SGALE will then forward the package to the SG6 IA Division. SG6 IA will validate that the IT system or IT component is Platform IT, while ensuring proper IA controls have been applied to the PIT. The SG PIT CA will review the package and issue a Determination Statement. The SG PIT DAA will review the information and the CA's determination and issue a PIT Approval Statement to the Program Management Office classifying the IT system or IT component as PIT or explaining that it is not PIT thereby issuing a non Approval Statement. The PIT Approval issued by the SG PIT DAA may be used by PM in lieu of Authority to Operate to prove compliance with C&A requirement.

6. Assessment Methods and Independent Testing

There are three assessment methods that can be applied to a Medical Platform IT; examine, interview, or test. All assessment methods will use the PIT IA Controls & Requirements from DoDI 8500.2 as tailored for Medical Systems. In general, the Mission Assurance Category III controls should be the starting point to develop the IA controls for Medical Systems.

To alleviate the potential for conflict of interest, testing must be conducted independently of developers and users in support of the PIT determination and approval. Medical PIT testing will be conducted by the SG PIT DAA IA Division, SG6. The testing method utilized will be based on the specific Medical PIT's design; in some cases the Defense Information Systems Agency's Medical Device, Security Technical Implementation Guide (STIG). If the Medical PIT cannot be tested with the STIG, an alternative test methodology will be used. The alternative test methodology will not preclude adequate test and/or evaluation of the Medical PIT, but will include all testable attributes of the Medical PIT.

Submitting Enterprise Wide PIT Request:

Via FEDEX to (unclassified):
AFMOA/SGALE
Attn: COTS Medical Device INFOSEC Program Office
693 Neiman Drive
Fort Detrick, MD 21702

Submit requests via e-mail to: https//medlog.detrick.af.mil
AFMOA/SGALE will provide the User Representative confirmation within three business days.

Submitting Site Specific PIT Request:
Via FEDEX to (unclassified):
AFMSA/SG6
ATTN: SG6 IA Division
Skyline 3 Suite 1500
Falls Church, VA 22104

Submit unclassified requests via e-mail to:
Note: Validation, CA determination and DAA approval process will apply to Site specific PIT Request.

7. Questions

User Representatives and vendors can refer questions about this appendix to the Office of Primary Responsibility, AFMSA/SG6 at DSN 761-6358, or AFMOA/SGALE at DSN 343-9081.

Appendix F

Platform IT Interconnection (PITI) Supplement

AIR FORCE
PLATFORM INFORMATION TECHNOLOGY INTERCONNECTION (PITI) GUIDE
VERSION 4.6
18 NOV 2010

DOCUMENT DISTRIBUTION RESTRICTIONS:
This document contains information exempt from mandatory disclosure under the Freedom of Information Act (FOIA). Exemption 3 applies.
Not Releasable to the Defense Technical Information Center per Department of Defense (DoD) Instruction 3200.12.
UNCLASSIFIED FOUO INFORMATION: THE DOCUMENT CONTAINS UNCLASSIFIED FOR OFFICIAL USE ONLY INFORMATION, WHICH IS FOR THE EXCLUSIVE USE OF GOVERNMENT AND CONTRACTOR PERSONNEL WITH A NEED-TO-KNOW THE INFORMATION. SUCH INFORMATION IS SPECIFICALLY PROHIBITED FROM POSTING ON UNRESTRICTED BULLETIN BOARDS OR OTHER UNLIMITED ACCESS APPLICATIONS.

This Page Intentionally Blank

Table of Contents

INTRODUCTION

Platform Information Technology (PIT) is a special category of an Information System (IS) that is embedded into, and essential for the operation of the systems mission. PIT is most often associated with a weapon system, but is equally applicable to any host Platform including training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapon systems, medical technologies, transport vehicles, buildings, and Supervisory Control and Data Acquisition (SCADA) systems. The need to protect and defend PIT by providing protections against breaches in confidentiality, integrity, availability, authentication, and non-repudiation, and the need to evaluate those protections, is often misunderstood or ignored in the development of PIT.

As part of a larger effort to improve the Air Force's (AF) Information Assurance (IA) Certification and Accreditation (C&A) process, SAF/XCD established an *Air Force Platform IT Working Group (PIT WG)* chaired by Air Force Material Command engineering leadership from Aeronautical Systems Center. The PIT WG is charged with identifying PIT IA issues and resolve them by developing guidance documents and policy recommendations. Initial focus areas were:

- The AF lacks clear IA implementation and compliance guidance for PIT and PIT Interconnection (PITI)
- Minimal guidance exists as to how to recognize PIT
- The AF lacks clear guidance on what authority can make a PIT determination

DoD IA policy (ref. a) specifically excludes weapons systems or other IT components, both hardware and software, that are physically part of, dedicated to, or essential in real time to a platform's mission performance where there is no PITI. Furthermore, PIT is not subject to the DoD IA C&A Process (DIACAP) (ref. b.). However, DoD Defense Acquisition Strategy (ref. c.) and AF Certification and Accreditation Program (AFCAP) (ref. d) require IA to be addressed in PIT system design and operation.

When a PIT system requires connection to a non-PIT system or network (i.e. system requiring DIACAP) in order to exchange information as part of the mission of the special purpose system, the IA requirements for the exchange must be explicitly addressed as part of the interconnection. This technical interconnection for network access to PIT is defined as a PITI in reference (a) E2.1.16.4. These interconnections are subject to DIACAP and AFCAP, focusing on the interconnection(s), not the PIT itself. IA controls, as defined in Reference (e) E2.1.26, are an objective condition of integrity, availability, or confidentiality. Because there is such diversity in

each potential application of IA controls for PITI's, it is crucial the DIACAP team be composed of appropriate stakeholders. The DIACAP team must consider flexibility when selecting the baseline IA controls applicable to the PITI(s) to protect both the PIT and non-PIT system or network, addressing both mission and community risk.

Reference e defines community risk as the probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population. For the purposes of this document, external networks, such as the Secure Internet Protocol Network (SIPRnet) and Non-Secure Internet Protocol Router Network (NIPRnet), represent the interacting population. All other controls are then to be considered to support mission requirements and are used to mitigate risk posed to the mission the system is intended to support.

Purpose

This document provides AF C&A process guidance on PITI IA implementation. It is intended to supplement existing DoD and AF Policy in the following areas:

- General information and clarifying the definition of a PITI
- Guidance on identifying a PITI
- Guidance on determining boundaries between a PIT and non-PIT system or network
- Guidance for connecting a PIT system to a non-PIT system or network using a PITI

This document does not detail the specific steps of the AFCAP process to obtain an Authority to Operate/Authority to Connect decision for a PITI. Please refer to most current AFCAP guidance for process requirements. This guide does not supersede connection requirements levied on a system from a Designated Approval Authority (DAA) outside of the AF provisioned portion of the Global Information Grid (GIG) for a connection to their network or system.

Applicability

This guidance applies to all Air Force military, civilian, and contractor personnel under contract by DoD who develop, acquire, deliver, use, operate, or manage Air Force information systems, including the Air National Guard and Air Force Reserve Command. The term Major Command, when used in this publication, includes Field Operating Agencies and Direct Reporting Units.

Program Managers (PM), Information System Security Engineers (ISSE), the Certifying Authorities (CA) or anyone working on their behalf, and DAA and their staff(s) will find this document particularly useful.

1.1 References

a. Department of Defense (DoD) Directive 8500.01E, *Information Assurance*, 24 Oct 02

b. DoD Instruction 8510.01, *DoD Information Assurance Certification and Accreditation Process*, 28 Nov 07

c. DoD Directive 5000.01, *The Defense Acquisition System*, 20 Nov 07

d. Air Force Instruction 33-210, *Air Force Certification and Accreditation Program* 23 Dec 08

e. DoD Instruction 8500.2, *Information Assurance Implementation*, 6 Feb 03

f. Air Force Policy Directive 33-2, *Information Assurance Program*, 19 Apr 07

g. Air Force Instruction 33-200, *Information Assurance Management*, 23 Dec 08

h. *C&A Guidance for Platform IT Interconnection* Naval Network Warfare Command Office of the Navy Operational Designated Accrediting Authority, Version 1.0, 20 Jan 09

i. CJCSI 6510.01E, *Information Assurance and Computer Network Defense*, 15 Aug 07

General Information

Complexity of a PITI varies with the nature of the interconnection. Full IA protection measures may be necessary when complicated systems are connected. In this case, it is appropriate to incorporate Internet Protocol routing, filtering, firewalling, intrusion detection, prevention, and other services. Fewer IA protection measures are necessary when simple systems or components are connected (e.g., a simple wind sensor connected to a navigation system). In this case, it is appropriate to consider hardware-enforced, one-way traffic flow (from sensor to navigation system) and a dedicated hardware link to the sensor as adequate IA protection. The sensor produces known, formatted data from a dedicated source and the navigation system is assured the information it receives has integrity from the very nature of the hardware interconnection. The general consideration should be assessing what risk does the PIT pose to the non-PIT? What risk does the Non-PIT pose to the PIT? In all cases, the protection of the GIG and its mission are paramount.

As part of a "Defense in Depth" strategy, using a well defined PITI as a measure to enhance security of the AF GIG is preferred. Some PITIs are solely in place to provide secured network

access to PIT devices. Others may have another primary role (for instance an accredited medical device with numerous modality PIT devices that serves as both a host system and secured network access).

In general, PITI is the interface where PIT connects to non-PIT. A DIACAP accredited system used as PITI must have the following three basic components:

- At least one external interface used to connect to a PIT system or network.
- Appropriate IA protection features serving to separate and protect PIT and the non-PIT
- Accreditation decision issued by a valid accreditation authority
- Authorization to Connect issued by the AF DAA or their designated representative

1.2 PITI Identification

PITI must utilize pre-determined baseline IA controls based on assigned Mission Assurance Category (MAC) and Confidentiality Level (CL) as required by DIACAP. These baseline IA controls can be found in the DIACAP Knowledge Service. Because it is ***essential*** to tailor the predetermined baseline IA controls in accordance with PITI system/operational requirements, a list of minimum recommended controls for mitigating the risk introduced to the GIG community from the PIT connection has been developed in Appendix A.

In accordance with reference c, additional IA controls:

> Selected should focus on the interconnection(s), not the PIT. Document any additional measures required of the external networks to extend IA services or to protect the PIT from interconnection risk.
>
> Must be selected as applicable and consider the MAC and CL of both the PIT and PITI.

The PM is required to ensure ISSE is accomplished and may assign an ISSE to the PITI system. The PM or the ISSE is responsible for determining the exact IA features that would provide adequate IA protection to both the PIT and the Non-PIT. Note: If the PITI does not have a PM or responsible entity assigned, the PM for the PIT must assume the responsibility for the PITI.

For new acquisition and systems seeking accreditation or reaccreditation, the fact that the system will be used as a PITI must be made clear in the DIACAP package. The DIACAP package for the system must explain the external interfaces used as PITI according to the provisions of section 2.1.1

When developing an IA Strategy for acquiring a PITI, the PM would be best served by considering type accredited solutions that are applicable to the connection requirements of the PIT. A type accredited system would allow that PIT PM to expedite the acquisition and fielding of the PIT capability as long as the preexisting PITI solution addresses the protection requirements for the PIT. Any deficiencies in the PITI solution would then have to be compensated for within the PIT design.

For systems with existing DIACAP accreditation, identification of one or more of the system's external interfaces to be used as PITI can be made by the system owner or PM and documented in the DIACAP package without reaccreditation, as long as, the existing interfaces do not need to be modified in a manner that negatively affects the security posture of the system serving as the PITI. A Minor Modification and/or a "Non-Negative Impact Statement" would have to be submitted by the Program Information Assurance Manager for the non-PIT.

The system owner or PM of both the non-PIT and PIT systems being interconnected, in coordination with Agents of the Certification Authority, Engineers, and IAMs, use the technical specification of the PITI solution to determine if the interface is suitable for use as PITI.

2.1.1 PITI Identification Process

The process of determining the IA controls applicable to a PITI system is the same as for all IS subject to DIACAP. Following this standard procedure:

- Determine MAC (i.e. I, II, or III) by PIT mission owner
- Determine CL (i.e. Public, Sensitive, or Classified)
- Consult reference (b) and Appendix A to determine the complete set of IA controls that apply to the system to address community risk based on its MAC and CL and identify the IA controls that:
  - Will be inherited—and state the source of inheritance
  - Will be implemented within the PITI
  - Are not applicable—and state the rationale in the Plan of Action and Milestones
- Assess each applicable IA Control for compliance
- Obtain PIT CA and DAA concurrence on the tailored baseline of IA controls

Note: At a minimum the IA controls selected for the PITI must address the risk posed to the community. The recommendation for these minimum controls is in Appendix A of this document. The controls can be implemented within the PIT, the identified PITI, or the hosting

enclave. All other controls are considered to mitigate risk to the mission and do not pose risk to the community if not implemented.

A DIACAP package for a PITI system must clearly identify the following:

- Specific external interface(s) being used as PITI
- Technical characteristics of each PITI external interface
- PIT systems and non-PIT systems to which each PITI interface connects

Every external interface must have a technical specification stated in the DIACAP package regardless of its use (i.e., PITI or not). The technical external interface specification includes, but is not limited to:

- Direction of data flow
- Classification of data
- Ports and protocols
- Technology used (e.g., Ethernet or serial; Transmission Control Protocol/Internet Protocol, User Diagram Protocol, etc.)

Once determined, the technical characteristics of an external interface used as PITI must be documented in the DIACAP package of the non-PIT system or network as well as in the corresponding documentation for the PIT system.

Whenever possible, all current and future PITI external connections should be documented in the accreditation package for that system as requirements for interfacing with other systems. If the interface currently exists, then a Memorandum of Agreement (MOA) may be needed. If an interface is established post-accreditation of the PITI, an MOA can be accomplished and appended to the existing documentation. Neither action should alter the security boundary of the PITI (i.e. forcing a reaccreditation decision/action).

2.1.2 PITI Demarcation

In determining the demarcation for a PITI, we must first understand the purpose for the PITI. For example, the PITI may simply provide an interconnection between the PIT and the non-PIT system or network. In many cases the PITI may also need to mitigate the risk to each system it interconnects. Depending on the need or pre-existing conditions, the PITI can range from a simple RJ45 cable connection to an entire enclave with a full boundary protection suite to accomplish this. Why the wide range? The PIT itself may not be able to implement IA controls,

and the owner of the non-PIT system or network may not be willing or able to modify their system/network to provide the protections needed by the PIT. The PITI may need to be designed to mitigate the risk (i.e., IA controls must be implemented in the PITI). These factors may drive not only the design of the PITI but also the demarcation between the PIT, the PITI, and the non-PIT system or network. The PITI may physically be part of or closely associated with the PIT. Architecture decisions of the PIT itself may be driven by the need for a simple or a complex PITI and the variety of non-PIT systems or networks to which the PIT must connect (e.g., Continental US connections may be relatively similar and may provide protections, but overseas locations with coalition partners may vary widely). The PITI may need to be designed as part of the PIT for all implementations, or the PIT and PITI may need to be distinct entities, such that the PIT may be connected with or without the PITI, depending on which IA controls the PIT or the non-PIT system or network may provide in any given implementation. Acknowledging the fact that PITI designs will vary greatly from use case to use case, the need to clearly identify the demarcation points between the systems accreditation boundaries is essential to the certification and accreditation efforts for both systems.

PITI Requirements (Functional)

MAC and CL determination for the PITI should be made by the PIT mission owner based on the mission impact the loss of the connection would pose to the success of the PIT's mission. The CL should be based on the classification of the information being transported and the classification of the network the PITI is connecting to. It is possible that the MAC of a PIT may be higher or lower than that of the PITI. An example of this is when a PIT has a true MAC I assignment, but relies on the PITI for only a portion of the mission capabilities that the PIT provides (network connectivity through PITI is a small percentage of mission need or capability). In this example, the PITI could be as low as a MAC III providing connectivity to the PIT.
If the PITI provides a controlled interface between two systems/networks of differing security classification, a cross domain solution is required.

If the MAC or CL of the PIT is lower than that of the connecting enclave, the enclave is responsible for assuring that the enclave's confidentiality, integrity, and availability are not degraded by the interconnection. The enclave hosting the PITI may be responsible for providing most of the physical and environmental controls for the PITI. As such, all controls that are inherited by the PITI must be clearly documented to ensure there are no unknown risks to PIT operations created by the PITI host enclave.

No PIT system should ever force a non-PIT system into an unplanned accreditation event, or otherwise impose additional IA or C&A costs on a non-PIT system at the non-PIT system's unfunded expense.

The basic premise of IA protection between the PIT and non-PIT domains is that there must be sufficient IA protections to guard the domains from each other. This includes such things as prevention of unwanted traffic from entering or exiting either domain (routing and firewalls); traffic flow control (inbound/outbound); intrusion monitoring/prevention (Intrusion detection systems (IDS)/ Intrusion Prevention System (IPS)); virus and malicious code prevention; ports, protocols and services management, etc.

Interfaces used as PITI are distinguished by the presence of IA devices, services or features that protect the PIT system and operational environment from non-PIT, and vice-versa. These IA features may include, but are not limited to:

- Firewalls and routers
- (IDS and IPS
- Other IA-enabled protection devices or software and procedures

Types of Interconnections

The following are examples of PIT interconnections to aid in identifying accreditation boundaries based on C&A governance. They are not intended to indicate ownership of PIT versus PITI.

Figure 1 shows the requirement for PITI between interconnected non-PIT and PIT systems. In this scenario, DIACAP would be required for the non-PIT and the PITI.

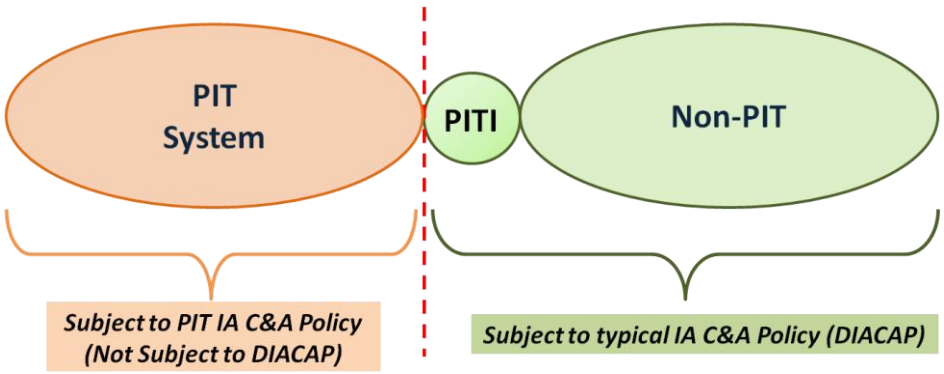


Figure 1: Non-PIT to PIT

Figure 2 shows the absence of the requirement for PITI between interconnected PIT systems. In this scenario, no DIACAP is needed for either PIT system or the Platform IT-to-Platform IT Interconnection (PTPI). The interface between connected PIT systems is called "PTPI." A

MOA and/or valid accreditation decision may be required, if this connection is made with different PIT authorization authorities, i.e. PIT DAAs, System DAAs etc

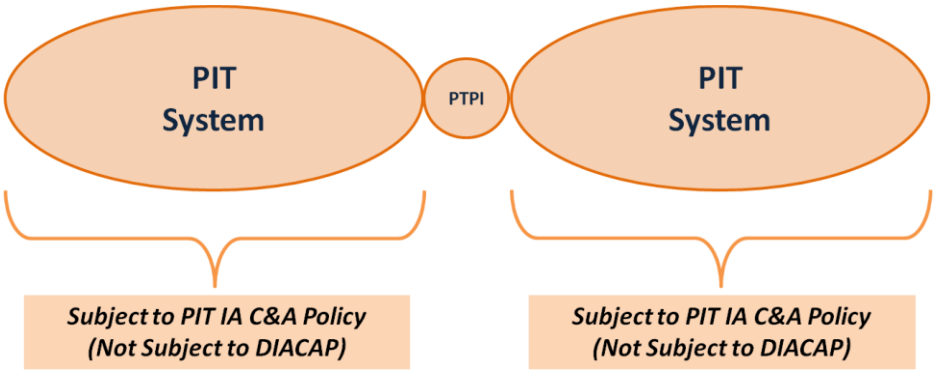


Figure 2: PIT-to-PIT Interconnection (PTPI)

When a PIT system connects to another PIT system in a more complex manner through an intermediate non-PIT system (such as the SIPRNet); DIACAP is required for each PITI that connects PIT to the accredited non-PIT network or system. Figure 3 shows the placement of PITI for this type of interconnection. Note: the connection between these PIT systems are not Virtual Private Network (VPN) tunneled or encrypted point to point.

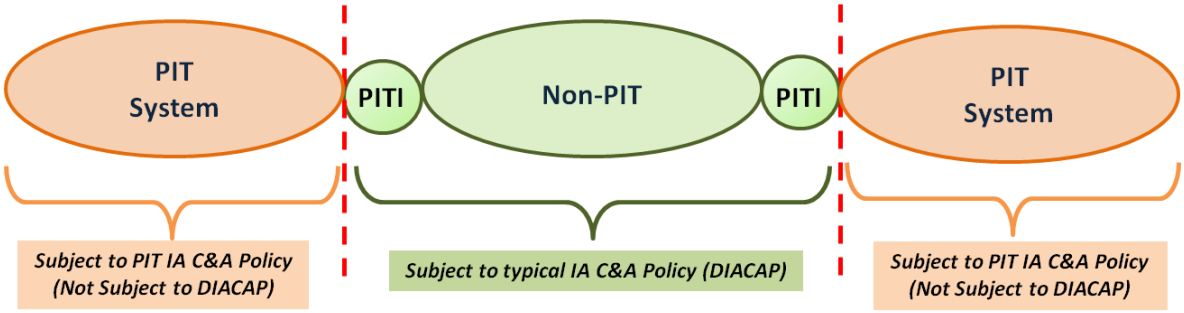


Figure 3: PIT Systems Connecting through an Intermediate Network or System

In figure 4 below, PIT-to-PIT interconnections that are tunneled/encrypted through a network (e.g. GIG) do not require DIACAP accreditation. These connections incorporate an encrypted VPN through approved solutions. Interactions with the network are not relevant, as the network only provides a transport function. MOAs are required per reference i for connection between different DAA's.

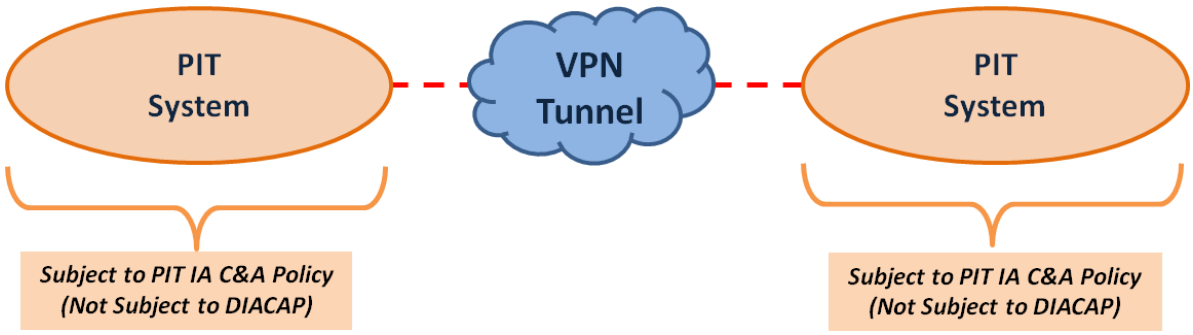


Figure 4: PIT Systems Connecting through a VPN

Memorandum of Agreement (MOA)

The PIT PM or system owner must develop an MOA for every PIT interconnection type, with only the following two exceptions:

Exception #1: The PM or system owner is the same for both the PIT and the non-PIT systems being interconnected.

Exception #2: All of the following are satisfied:

- The non-PIT system, together with its advertised external connection that will be used to connect to PIT systems, offers IA protection required for meeting the needs of the PIT interconnection
- The non-PIT system's accreditation package is approved by a DAA with a statement identifying the system (or a portion of it) as PITI, including a full description of the technical IA protections offered by the system and its PITI external interface
- Both the PIT and non-PIT PM/system owner, in conjunction with their respective DAA or agents acting on their behalf, agree these provisions are satisfied without an MOA

A PITI MOA must explain the technical nature of the interconnections. It must contain at least the following four components:

- Roles and responsibilities for all PIT stakeholders and relationship with respective PITI(s)
- Identification of the interface(s) being used (both PIT and non-PIT sides)
- Specification of the IA features that separate the PIT domain from the non-PIT domain
- Statement of IA risk for the PIT system being connected to the PITI

Additionally, the PMs or system owners involved may want to include a section that specifies which PM will assume the financial responsibility for C&A of the PITI. This would be appropriate if the PIT PM/system owner is to assume all or part of that responsibility.

In addition to an MOA, a PITI PM may require some form of a Service Level Agreement (SLA) or an Interconnection Security Agreement for establishing a connection agreement between a PITI and a non-PIT system or network.

SLAs define division of responsibilities for network operations and services to minimize duplication of effort between organizations. MOAs define the resources each party will provide to support delivery of negotiated services. SLAs quantify the level of support for the services defined in an MOA. SLAs identify the minimum levels of support required by the users rather than acceptable failure rates. SLAs also describe the prioritization of systems and services.

ISAs are drafted for sites using a service provider other than the regular services provided within your base such as the NIPRNet, SIPRNet, and Joint Worldwide Intelligence Communications System. Those service providers can include but are not limited to Joint Forces Joint Training and Experimentation Network, Missile Defense Agency's CNet, Defense Research and Engineering Network, and Distributed Mission Operations Network.

Platform IT Interconnection Scenarios

This section explains three, more complex PITI scenarios.

Scenario 1: An Existing DIACAP Accredited System Serving as the PITI

This scenario uses a previously certified and accredited non-PIT system as a PITI (e.g. enclave or existing type accredited PITI). The system has one or more external interfaces that are documented and identified in its DIACAP package that provides both a general set of technical characteristics for the external interface, as well as, technical specification allowing it to be used as PITI.

Using the interface's technical specification documented in the DIACAP package for the non-PIT system, the PIT systems may connect to the interface as long as they meet the technical specifications and security requirements of the non-PIT system.

In most cases, an MOA is established between the Information System Owners or PM for the PIT and non-PIT systems. The MOA clearly explains the expectations and responsibilities of each entity and is entered as an artifact in the accreditation packages of both the PIT and non-PIT system.

Unless modified by an MOA, responsibility for C&A of the PITI in this example is with the non-PIT system owner or PM.

Figure 5 shows a PIT system using an existing, suitable, previously accredited PITI.

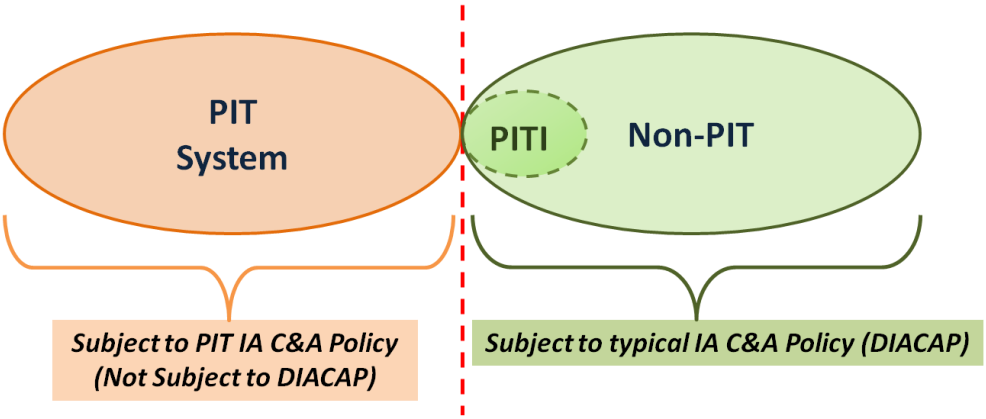


Figure 5: An Existing System with Accreditation is the PITI (MOA required)

Scenario 2: A Portion of the PIT System becomes the PITI

A PIT system contains the IA protections necessary for PITI on one of its interfaces and desires connection with a non-PIT system that does not have an interface suitable for PITI. Since the PIT system is not subject to DIACAP, it may not meet the C&A requirement for PITI. The non-PIT system owner or PM is unwilling or unable to upgrade the non-PIT system to certify it as a PITI, and is unwilling or unable to enter into an MOA with the PIT system owner or PM, per Scenario #1.

In this case, the PIT system or component owner or PM may elect to remove a portion of the PIT system from the PIT boundary, create an accreditation boundary for it, and have it certified and accredited under DIACAP as a PIT Interconnection.

The removed components form a new system that is considered to be the PITI. There will be at least two external interfaces out of this PITI's accreditation boundary; one is with the non-PIT system to which connection was originally desired or established (an accredited external interface for both systems), and the other is with the PIT system.

Responsibility for C&A of the new PITI system is with the PIT system owner. The PITI accreditation documentation and accompanying ATO should be referenced in the non-PIT accreditation package.

Figure 6 shows a portion of the PIT system (orange) removed from the PIT boundary, made into a new system designated as PITI and accredited (green), which then is able to connect both to the non-PIT system (green) and the PIT system (orange).

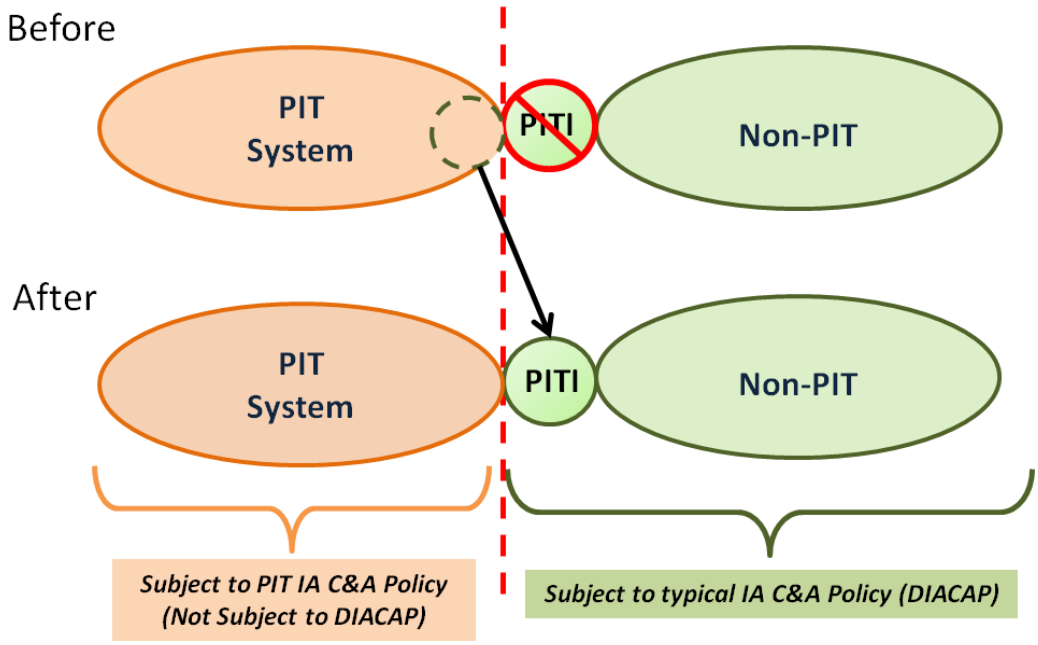


Figure 6: A Portion of the PIT System Becomes the PITI

Scenario 3: A Third Party Provides the PITI

If neither the PIT nor the non-PIT system owner or PM is willing or able to provide the PITI, the PIT PM may make arrangements with a third party to provide a system that will fit between the two systems and serve as the PITI. This system has its own accreditation boundary, at least two external interfaces (one with the PIT system and the other with the non-PIT system), and its own accreditation.

In accordance with the provision of the MOA, responsibility for C&A of the PITI system is with the third party. The PIT and third party PITI PM will develop and include the interconnection in their respective accreditation packages.

Figure 7 shows a PIT system (orange) connecting through a third party provided PITI system (green) to a non-PIT system or network (green).

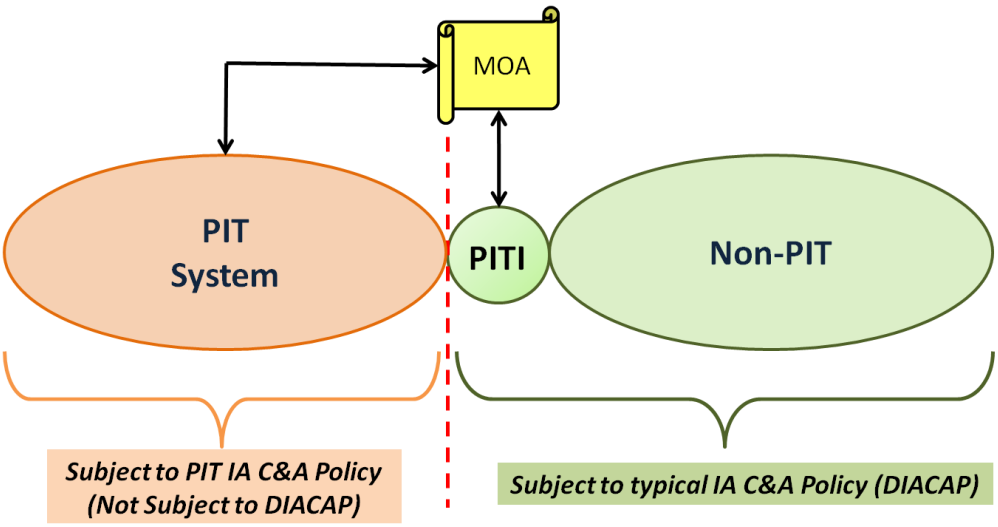


Figure 7: A Third Party Provides the PITI

NOTE: PITI systems that are SCI do not follow DIACAP but follow ICD 503 with AFISRA, as the accreditation authority, providing the ATO. The AF-DAA still provides the ATC.

Appendix A

Recommended Controls to Address Community Risk

PITIWG recommendation for I

ACRONYM	DEFINTION
AF	Air Force
AFCAP	Air Force Certification and Accreditation Process
ATO	Authority to Operate
C&A	Certification and Accreditation
CA	Certifying Authority
CL	Confidentiality Level
DIACAP	DoD Information Assurance Certification and Accreditation Process
DoD	Department of Defense
IA	Information Assurance
IAM	Information Assurance Manager
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISSE	Information System Security Engineer
IT	Information Technology
MAC	Mission Assurance Category
MOA	Memorandum of Agreement
ODAA	Operational Designated Accrediting Authority
PIT	Platform Information Technology
PITI	Platform Information Technology Interconnection
PM	Program Manager
PTPI	Platform IT to Platform Interconnection

Definitions

Platform IT Interconnections refer to network access to platform IT and has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Examples of platform IT interconnections that impose security considerations include, but are not limited to: communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration. Source AFI 33-210.

Platform IT is considered a special purpose system which employs computing resources (i.e., hardware, firmware, and optionally software) that are physically embedded in, dedicated to, or essential in real time to the mission performance. It only performs (i.e., is dedicated to) the information processing assigned to it by its hosting special purpose system (this is not for core services). Examples include, but are not limited to: SCADA type systems, training simulators, diagnostic test and maintenance equipment. Source AFI 33-210.

Acknowledgements

The creation of a document of the size, scope, and far-reaching impact of the PITI Guide would be impossible without the contributions of a great many talented and dedicated people. I wish to express my sincere thanks to the following individuals who participated during the documents development, review, and approval process and contributed in immeasurable ways.

Raju B. Patel, Ph.D.
IA/AT Technical Advisor
ASC/ENAS

Troy Allison
Aeronautical Systems Center
Capt Kenneth Carmichael
Air Combat Command
Eric Butner
MITRE Corporation
MSgt David Griffith
Air Force Special Operations Command
Samuel Langham
Air National Guard
Maj Mike Maes
AF Operation Test and Evaluation Command
LtCol Sean Murphy
Air Force Medical Operations Agency
Mark Metea
MITRE Corporation
Richard Booth
Air Education and Training Command
Douglas Wedel
Aeronautical Systems Center
John Sward
USAF Distributed Mission Operations Center
David Simon
Aeronautical Systems Center
Randy Gabel
MITRE Corporation
Paul Manning
Air Combat Command
Mathieu Cloutier
Electronic Systems Command

Appendix G

Platform Information Technology (PIT) Information Assurance

Assessment Criteria Tables: Means, Opportunity, Impact and Criticality

Appendix G

Platform Information Technology (PIT) Information Assurance

Assessment Criteria Tables: Means, Opportunity, Impact and Criticality

Reference: Information Assurance (IA) Risk Assessment (IARA) Process for Military Systems White Paper, Deborah Williams and Larry Johnson, PhD, www.sentar.com

Table 1: Means		
Level	**Column A: Direct IA Impact for Subject Areas:** **Identification and Authentication (IA)** **Enclave and Computing Environment (EC)** **Enclave Boundary Defense (EB)**	**Column B: Indirect IA Impact for Subject Areas:** **Security Design & Configuration (DC)** **Physical and Environmental (PE)** **Personnel (PR)** **Continuity (CO)** **Vulnerability and Incident Management (VI)**
M-1	Adversary's Difficulty: • Requires deliberate effort and elevated privileges, and • Requires vulnerability "linking" of multiple vulnerabilities for exploit to occur, and • Requires introduction of new code or script onto system and significant system time to link conditions that facilitate and execute the exploit, and • Mounting/attack would take considerable time and would be visible to IDS and/or auditing	Programmatic: • Organizationally approved policies/other programmatic guidance exists, and • Programmatic guidance addresses relevant IA requirements but is outdated, but • Responsible authorities for computing enclave or location has up-to-date local SOP/procedures that provide at least partial compensation Or, Environmental: • Organizationally approved guidance exists, and • Responsible authorities for computing enclave or location has valid SOP/approach to meeting environmental control requirement, and • Equipment is functional, but • Some required maintenance/system checks are out-of-date Or, Physical/Administrative: • Organizationally approved guidance exists, and • Responsible authorities for Computing Enclave or location have adequate local SOP/process for meeting physical/administrative security requirement, and • Process is implemented, and • Equipment is functional, but • Minor discrepancies are observed in records-keeping/paperwork
M-2	Adversary's Difficulty : • Exploiter must execute exploit of one or more vulnerabilities, and • Requires deliberate effort and elevated privileges, and • Pathway to elevated privileges exists, and • Vulnerability is known, and vulnerability "linking" is not required, but	Programmatic: • Organizationally approved programmatic guidance exists, and • Guidance inadequately or incorrectly addresses one or more IA requirements, or • Implementation of guidance is not effective, and • Component SOPs/processes adequately implement the programmatic guidance but

	• New attack mechanism/exploit script/code would have to be created and mounted onto system, and • Attack mechanism/script, once created, can be mounted and executed rapidly (i.e., speed of mounting and execution would likely prevent successful SA/NA response, with or without IDS or audit logging/review) Or, Adversary's Difficulty: • Requires linking of multiple vulnerabilities, and • Would require only a minor modification of the attack mechanism/script to "link" the vulnerabilities for exploit, and • Attack mechanism/script must be mounted onto system, and • Mounting/attack would take considerable time and would be visible to IDS and/or auditing	• Component SOPs/processes contain the same deficiencies as the programmatic guidance Or, Environmental/Physical/Administrative: • Approved programmatic guidance exists and is adequate, but • Component SOP for implementing guidance fails to address one or more parts of the programmatic guidance, Or, • Component SOP for implementing guidance is adequate, but • Actual execution is only partially implemented Or, • One or more pieces (but not all) of required environmental, physical security or administrative security equipment is absent and/or is dysfunctional
M-3	Adversary's Difficulty: • Exploiter must execute exploit of one or more vulnerabilities, and • Requires deliberate effort and elevated privileges, and linking of vulnerabilities is not required for exploit, and • Pathway to elevated privileges exists, and • Exploit is widely known, and • Attack mechanism/"canned" exploit script is available, but • Attack mechanism/script would have to be modified for exploit, and • Attack mechanism/script must be mounted onto system, and • Attack mechanism/script, once modified, can be mounted and executed rapidly (i.e., speed of mounting and execution would likely prevent successful SA/NA response, with or without IDS or audit logging/review)	Programmatic: • Organizationally-approved programmatic guidance exists, but • Organizationally-approved programmatic guidance has not been implemented, and, • Organizationally approved guidance fails to address (i.e., omits) one or more IA requirements, and • Local SOPs are out-of-date and/or fail to compensation for the omission(s) in organizationally approved guidance Or, Environmental/Physical/Administrative: • Organizationally approved guidance exists but • Organizationally approved guidance fails to address (i.e., omits) one or more IA requirements, and • Responsible Authorities for computing enclave or locations SOPs adequately implement provided Organizationally approved guidance but omit the same IA requirements, and • One or more pieces (but not all) required environmental, physical security or administrative security equipment is absent and/or is dysfunctional
M-4	Adversary's Difficulty: • Exploiter must execute exploit of one or more vulnerabilities, and • Requires deliberate effort and elevated privileges, and • Pathway to elevated privileges exists as part of vulnerability, and • Exploit is widely known, and linking of vulnerabilities is not required for exploit, and • Attack mechanism/"canned" exploit script is widely available and requires no modification for exploit, but	Programmatic: • PD-approved programmatic guidance does not exist, and • Local component SOPs/procedures exist but do not adequately compensate for lack of guidance and fail to meet some (but not all) IA requirements Or, Environmental/Physical/Administrative: • Organizationally approved guidance does not exist, and • Responsible authorities for computing enclave or location have developed SOPs/implementing procedures, but are marginally adequate, and • One or more pieces (but not all) required environmental,

	• Attack mechanism/script must be mounted onto system, and • Attack mechanism/script can be mounted and executed rapidly (i.e., speed of mounting and execution would likely prevent successful SA/NA response, with or without IDS or audit logging/review) or • Vulnerability can be exploited without the addition of new code or script (e.g. exploit of permissive file settings and access control parameters)	physical security or administrative security equipment is absent and/or is dysfunctional
M-5	Adversary's Difficulty: • Exploiter must execute exploit of one or more vulnerabilities, and • Exploit could be performed accidentally by any authorized user/account holder Or, Adversary's Difficulty: • Involves one or more vulnerabilities, and • Exploit/attack mechanism is widely known, and • Requires deliberate effort, and • Does not require elevated privileges, and • Does not require any "exploit script", and • Could be performed by any authorized user/account holder Or, Adversary's Difficulty: • Involves vulnerability that affords unauthorized access by an outsider, and • Could be performed by such an individual if access were gained	Programmatic: • Organizationally -approved programmatic guidance does not exist, and • Responsible authorities for computing enclave or location have not developed and/or implemented SOPs/procedures. Or, Environmental/Physical/Administrative: • Organizationally approved guidance does not exist, and • SOPs/implementing procedures developed by either responsible authorities for the computing enclave or location do not exist Or, • All required environmental, physical, or administrative security equipment is absent or dysfunctional

Table 2: Opportunity		
Level	**Column A: Direct IA Impact for Subject Areas:** **Identification and Authentication (IA)** **Enclave and Computing Environment (EC)** **Enclave Boundary Defense (EB)**	**Column B: Indirect IA Impact for Subject Areas:** **Security Design & Configuration (DC)** **Physical and Environmental (PE)** **Personnel (PR)** **Continuity (CO)** **Vulnerability and Incident Management (VI)**
O-1	Adversary's Access: • Is limited to a single System computing enclave (workstation, server, or LAN), and no pathway into the System exists from the System's LAN, WAN or external system or network, Or • Is limited to a single System computing enclave, and pathway into the System enclave exists, but System enclave is protected from the System's LAN, WAN and all external networks and systems by internal System enclave boundary protective devices. (e.g. system	Opportunity for Occurrence: • Is limited to a single computing enclave existing at a singular location, and • Does not exist for the remainder of the other computing enclaves at that location (i.e., no exploit path is opened from one computing enclave to another)

	enclave includes firewalls or other protection devices or mechanisms.)	
O-2	Adversary's Access: • Is limited to a single System computing enclave, and • Pathway exists into the System computing enclave from outside via the System's LAN or WAN , and • System enclave does not have boundary protective devices at its internal interface, but • has effective/properly configured external interface boundary protective devices (i.e., only an insider has a potential exploit opportunity, and it only against a single System), and • System enclave has effective/properly configured interface boundary protective devices to all other external interfaces to only legitimate and known connected systems, (if any) and, well documented assessments exist that validate the status of inter-connections.	Opportunity for Occurrence: • Is limited to a single physical location that exists within a geographically distributed network, but • Exploit could affect (or has the potential to affect) more than one computing enclave at that singular location.
O-3	Adversary's Access: • Is limited to a single System enclave, and • Pathway exists into the System enclave from outside via the WAN, and • System enclave has no (or ineffective/incorrectly configured) boundary protective devices at its interface, and • System has no (or improperly configured) WAN interface boundary protective devices (i.e., Insiders within connected systems have potential to gain entry into System enclave.) Or: Exploiter's Access: • Is limited to a single System enclave, and • Pathway exists between the System enclave and a separate system (e.g., a legitimately connected system, test system, etc.), and • System enclave has no (or improperly configured) protective devices with one or more of its external non- interfaces (i.e., a connected" system's insider has a potential exploit opportunity against a single System across the interface boundary)	Opportunity for Occurrence: • Is not limited to a single location within the geographically distributed computing network (i.e., problem exists at two or more locations) Or, • Exploit of vulnerability would likely occur at multiple locations within the geographically distributed computing network.
O-4	Adversary's Access: • Is available through the System's WAN (i.e., on the WAN IP address space; exploit opportunity exists against or across the WAN itself), and • Is available through the absence of (or improperly configured) interface boundary protective devices at one or more of its internal System interfaces (i.e., any insider on one or more System LANs has a potential exploit	Opportunity for Occurrence: • Exploit of vulnerability would likely occur across multiple locations of a geographically distributed computing network, but • Condition in and of itself does not create a potential exploitation path to other locations of the geographically distributed computing network.

	opportunity across the to another System(s) and against the WAN itself), but • Is impeded through an effective/properly configured boundary protective devices at all external interface boundaries	
O-5	Adversary's Access: • Is available through the System's WAN (i.e., on the WAN IP address space; exploit opportunity exists against or across the WAN itself), and • Is not restricted based on the presence of interface boundary protective devices, or interface boundary protective devices are improperly configured; or interface boundary protective devices at one or more of its internal System interfaces is absent or insufficient to guard against a potential exploit stemming from the WAN and/or legitimately connected systems and /or: • Is not restricted based on the presence of interface boundary protective devices, or improperly configured interface boundary protective devices at one or more of its external interface boundaries (i.e., an outsider has a potential exploit opportunity).	Opportunity for Occurrence: • Has the potential to be exploited across the entire geographically distributed computing network, and • Has a potential exploitation path into or out of the computing network to other networked systems.

Table 3: Impact		
Level	**Column A: Direct IA Impact for Subject Areas:** **Identification and Authentication (IA)** **Enclave and Computing Environment (EC)** **Enclave Boundary Defense (EB)**	**Column B: Indirect IA Impact for Subject Areas:** **Security Design & Configuration (DC)** **Physical and Environmental (PE)** **Personnel (PR)** **Continuity (CO)** **Vulnerability and Incident Management (VI)**
The following DIACAP Knowledge Base Impact Code impact code descriptions are applicable to this table: **Low:** Exploitation of the risk may result in temporary loss of information resources and/or limit the effectiveness of mission capability and may have a limited adverse effect on system operations, management, or information sharing. **Medium:** Exploitation of the risk may result in loss of information resources and/or the significant degradation of mission capability and may have a serious adverse effect on system operations, management, or information sharing. **High:** Exploitation of the risk may result in the destruction of information resources and/or the complete loss of mission capability, and may have a severe or catastrophic effect on system operations, management, or information sharing.		
I-1	Non Compliant Control Rating: • Tool Rating: Low (or equivalent) (if applicable), and • DIACAP Knowledge Base Impact Code: Low.	Non Compliant Control Rating: • DIACAP Knowledge Base Impact Code: Low. OR All applicable control provisions can be met with the NIST low-baseline application
I-2	Non Compliant Control Rating: • Tool Rating: Medium/High (or equivalent) (if applicable), and	Non Compliant Control Rating: • DIACAP Knowledge Base Impact Code: Low Or,

	• DIACAP Knowledge Base Impact Code: Low or • Tool Rating: Medium/High (or equivalent) (if applicable), and • DIACAP Knowledge Base Impact Code: Medium, but complementary protective measures exist that mitigate impact of exploit.	• DIACAP Knowledge Base Impact Code: Medium, but complementary protective measures exist that mitigate impact of exploit
I-3	Non Compliant Control Rating: • Tool Rating: Low/Medium (or equivalent) (if applicable), and • DIACAP Knowledge Base Impact Code: Medium.	Non Compliant Control Rating: • DIACAP Knowledge Base Impact Code: Medium
I-4	Non Compliant Control Rating: • Tool Rating: High (or equivalent) (if applicable), and • DIACAP Knowledge Base Impact Code: Medium or • Tool Rating: High (or equivalent) (if applicable), and • DIACAP Knowledge Base Impact Code: High, but complementary protective measures exist that mitigate impact of exploit or NIST defined medium baseline control measures are applicable, but protective measures exist that mitigate impact of exploit.	Non Compliant Control Rating: • DIACAP Knowledge Base Impact Code: Medium or • DIACAP Knowledge Base Impact Code: High, but complementary protective measures exist that mitigate impact of exploit
I-5	Non Compliant Control Rating: • Tool Rating: Low/Medium/High (or equivalent) (if applicable), and • DIACAP Knowledge Base Impact Code: High.	Non Compliant Control Rating: • DIACAP Knowledge Base Impact Code: High

Table 4: Criticality		
Level	**Column A: Direct IA Impact for Subject Areas:** **Identification and Authentication (IA)** **Enclave and Computing Environment (EC)** **Enclave Boundary Defense (EB)**	**Column B: Indirect IA Impact for Subject Areas:** **Security Design & Configuration (DC)** **Physical and Environmental (PE)** **Personnel (PR)** **Continuity (CO)** **Vulnerability and Incident Management (VI)**
C-1	Exploit consequences: • Are limited to a single system within a defined computing enclave, and exploit could impair that system's ability to provide required measures of availability, confidentiality or integrity for a short time; but the short term loss of availability, confidentiality or integrity could not impede the required attributes of availability, confidentiality or integrity across the system or network as a whole. Or, Exploit consequences: • Could impede the required attributes of availability, confidentiality or	Exploit consequences: • Would have the potential to impair or disrupt the functionality of a single system or computing enclave at one location , and • Would have little to no impact on the system's or network's ability to perform its operational mission Or, • Would have the potential to impair functionality of a the affected system(s) / network at one location , but • Complimentary/compensating procedures are in place to prevent/mitigate exploit consequences

	integrity across the system or network as a whole, but • Complimentary and effective safeguards are in place to prevent/mitigate exploit	
C-2	Exploit consequences: • Are limited to a single system within a defined computing enclave, and exploit could impair that system's ability to provide required measures of availability, confidentiality or integrity for a short time; but the short term loss of availability, confidentiality or integrity is unlikely to impede the required attributes of availability, confidentiality or integrity across the system or network as a whole.	Exploit consequences: • Would have the potential to impede operational functionality of a critical part of the system / network, but • Is unlikely to result in near-term catastrophic operational failure of the system / network itself.
C-3	Exploit consequences: • Are limited to a single system or multiple systems within a defined computing enclave, and exploit could impair those system's ability to provide required measures of availability, confidentiality or integrity for a short time; and the short term loss of availability, confidentiality or integrity may possibly impede the required attributes of availability, confidentiality or integrity across the system or network as a whole; but such an impediment is unlikely to result in operational impacts to the system(s) or network as a whole. Or, • Could impact the entire network or system's ability to provide required measures of availability, confidentiality or integrity for a short time, but • the overall operational mission of the system is unlikely to be impeded, and alternative measures are in place that provide for a work-around should the system be unavailable for a short time.	Exploit consequences: • Would have the potential to result in catastrophic near-term failure of a single critical computing system(s) , computing enclave(s) at one or more locations, but • Overall operational mission capability would be minimally impeded.
C-4	Exploit consequences: • May be limited to a single system or computing enclave, but that single system / computing enclave is critical to the operational mission of the system(s) / network. and impeded capabilities to provide required measures of availability, confidentiality or integrity could extend beyond a short time, or impeded measures of availability, confidentiality or integrity for even a short time are likely to adversely impact the overall operational mission of the system(s)/ network. Or, • Could impact the entire network or system's ability to provide required	Exploit consequences: • Would be limited to a single system / computing enclave / network at one or more locations; and • Could result in near-term catastrophic failure of that system/ computing enclave / network, and • Could impede the operational mission of the system itself.

	measures of availability, confidentiality or integrity for a short time, and • It is possible that the impediment of required levels of availability, confidentiality or integrity will impede the overall operational mission of the system(s) / network. and alternative measures could be developed that would provide for a work-around should the system be unavailable for a short time.	
C-5	Exploit consequences: • Will impact multiple systems / computing enclaves / networks that are critical to the operational mission of the system(s) / network. and impeded capabilities to provide required measures of availability, confidentiality or integrity for even a short time are very likely to adversely impact the overall operational mission of the system(s) / network.	Exploit consequences: • Have the potential to significantly operationally impact one or more operationally critical systems/ computing enclaves / networks spanning multiple locations and • Has the potential to result in the significant impediment of the operational mission of the overall system.